SIEVERS
Security & Network

Solutions

SIEVERS
all digital.

SIEVERS Security & Network Solutions
2024, Q4, 1. Auflage

all digital.

Security & Network

powered by protection –
driven by innovation.

SIEVERS

Von der Beratung über die Lösung in den Betrieb – mit der SIEVERS-GROUP

Die Aktivitäten der acht operativen Business-Units folgen einem bewährten Geschäftsmodell, das aus drei miteinander korrelierenden Säulen besteht: Beratung – Lösung – Betrieb. Perfekt aufeinander abgestimmt, schaffen sie die bestmöglichen Voraussetzungen, um gemeinsam mit Ihnen den rasanten Wandel hin zu digitalen Geschäftsmodellen, Cloud-Technologien und neuen Formen der Zusammenarbeit voranzutreiben, indem wir

Beratung

Ihr Unternehmen und sein Umfeld im Hinblick auf Ihre firmenspezifische IT-Strategie ganzheitlich betrachten,

Lösung

Hard- & Software zu einzigartigen IT-Lösungen kombinieren, um sie perfekt auf Ihre Anforderungen abzustimmen, und

Betrieb

Ihren IT-Betrieb professionell betreiben, damit Sie sich voll und ganz auf Ihr Kerngeschäft konzentrieren können.

Gestalten Sie mit uns die Zukunft Ihres Unternehmens!

all digital.

Liebe Leserin, lieber Leser,

Ihre IT ist das Rückgrat Ihres Unternehmens – höchste Sicherheitsstandards sowie Stabilität und Verfügbarkeit Ihrer IT-Umgebung sind dafür unabdingbar. Moderne Unternehmen müssen sich nicht nur gegen die wachsende Zahl an immer komplexeren Cyberangriffen schützen, sondern auch auf leistungsfähige und flexible IT-Lösungen setzen, die ihre Geschäftsprozesse optimal unterstützen, Sicherheit bieten sowie Innovation und Wachstum ermöglichen.

Genau das bieten wir Ihnen mit unserem breit aufgestellten Produkt- und Serviceportfolio in den Bereichen IT-Security und Netzwerkinfrastruktur: Unsere Security-Lösungen schützen Ihre Daten und Systeme zuverlässig vor aktuellen Bedrohungen und zukünftigen Risiken, während unsere Netzwerkprodukte für reibungslose Verbindungen und eine skalierbare Infrastruktur sorgen. Basierend auf modernsten Technologien und praxisbewährten Konzepten lassen sich unsere Lösungen nahtlos in Ihre bestehende IT-Landschaft integrieren. Dabei setzen wir auf einen ganzheitlichen Ansatz: Wir betrachten nicht nur die technische Seite, sondern auch Ihre Geschäftsprozesse sowie individuelle Anforderungen, um Sie bestmöglich zu unterstützen.

Einen 100%igen Schutz vor IT-Bedrohungen oder -Ausfällen gibt es zwar nicht – dennoch können wir Ihre IT-Landschaft ein ganzes Stück weit widerstandsfähiger machen. Unser Job ist erst dann getan, wenn Sie sich sicher und souverän in der digitalen Welt bewegen und agieren. Lassen Sie uns das gemeinsam anpacken!

Michael Saak

Head of Security & Network
SIEVERS-SNC Computer & Software GmbH & Co. KG
Ein Unternehmen der SIEVERS-GROUP

Security & Network-Team

Head of Security & Network

Michael Saak
msaak@sievers-group.com
+49 (541) 9493-41793

Unser Sales-Consultant-Team

Louisa Hehmann
lhehmann@sievers-group.com
+49 (541) 9493-4474

Christoph Hein
chhein@sievers-group.com
+49 (541) 9493-5241

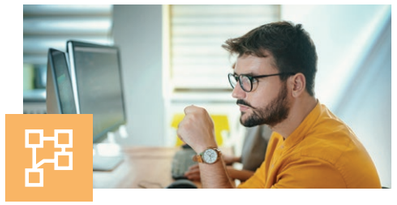
Adam Markwiok
amarkwiok@sievers-group.com
+49 (541) 9493-5330

Sebastian Oetzel
soetzel@sievers-group.com
+49 (541) 9493-41970

Maike Werth
mwerth@sievers-group.com
+49 (541) 9493-41936

Inhalt

Security



Network

Security

Die Digitalisierung unserer Wirtschaft bringt auch ihre Schattenseiten mit sich: IT-Systeme müssen geschützt werden. Das verantwortungsbewusste Schützen Ihrer IT-Systeme vor Schäden und Bedrohungen definiert IT-Security, IT-Sicherheit oder auch Informationssicherheit. Zu schützen sind einzelne Dateien, Computer, Netzwerke, Cloud-Dienste bis hin zu ganzen Rechenzentren. Dazu kommen Cybergefahren – von APts und Malware über Spam, Phishing und Ransomware bis zu DDoS-Angriffen –, die durch Cybersecurity verhindert werden. Heutzutage sind die meisten Systeme mit dem Internet verbunden, daher lassen sich die Begriffe IT-Security und Cybersecurity gleichsetzen. Fazit: Der Schutz der IT-Systeme vor Ausfall und die notwendige Belastbarkeit der IT-Systeme sind grundlegend für die Aufrechterhaltung einer Business Continuity.

Die Vorteile einer IT-Security für Ihr Unternehmen:

- Schutz vor Cyberangriffen
- Schutz Ihres Know-hows
- Sicherheit für Ihre Kunden
- Schnelle Reaktionsfähigkeit
- Zusammenführung von Menschen, Prozessen und Technologien

Neben der rein technischen Absicherung sorgen wir für ein angemessenes Maß an organisatorischer Sicherheit. Nur wenn die technischen Maßnahmen mit den organisatorischen im Einklang stehen und sich die Waage halten, wird ein hohes Niveau an Informationssicherheit erreicht.

Unsere IT-Security-Leistungen für Sie:

- Governance, Risk & Compliance
- Application Security
- Cloud Security
- Cyber Crime & Defence
- Datacenter Security
- Infrastructure- und Perimeter-Security
- Workplace Security

Information Security Management System

SIEVERS NIS-2 Kompass

Sie vermuten, dass Sie von der NIS-2-Richtlinie betroffen sind oder arbeiten eng mit betroffenen Unternehmen zusammen? Lassen Sie uns gemeinsam durch die zahlreichen Aspekte der Richtlinie navigieren: In unserem eintägigen Workshop zu dem Thema, dem NIS-2 Kompass, ermitteln wir gemeinsam und individuell den Status quo Ihrer Organisation – sowie die Maßnahmen, welche Ihnen zur Erfüllung der gesetzlichen Anforderungen fehlen.

Der Workshop ist auf einen Tag ausgelegt. Hierfür treffen wir uns bei Ihnen vor Ort oder auf Wunsch auch gerne remote über Microsoft Teams. Innerhalb einer einleitenden etwa dreistündigen Kick-off-Präsentation werden alle Teilnehmenden umfassend über die Anforderungen der NIS-2-Richtlinie informiert. Daran schließt sich ein dreistündiges Interview an, in dem gemeinsam der Status quo Ihrer Organisation eruiert sowie individuelle und notwendige Maßnahmen zur Erfüllung der gesetzlichen Vorgaben in der gemeinsamen Runde diskutiert werden.

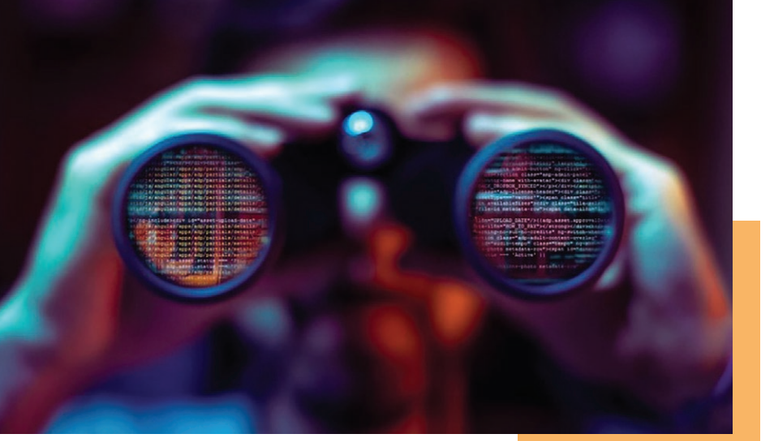
Damit wir uns einen Überblick über die IST-Situation Ihrer Organisation machen können, sollten folgende Positionen im Rahmen des NIS-2 Kompass vertreten sein: IT-Leitung, IT-Administration, Informationssicherheitsbeauftragte:r (falls vorhanden), Mitglied der Geschäftsführung sowie Vertreter der Personalabteilung. Darüber hinaus ist es Ihnen freigestellt, weitere Mitarbeitende, die für das Thema sensibilisiert werden sollen, zu dem Workshop einzuladen.

Im Anschluss erhalten Sie eine Übersicht der Ergebnisse des Workshops sowie eine Orientierungshilfe zur Umsetzung von Handlungsempfehlungen im Rahmen der NIS-2-Anforderungen.

Ihr Nutzen

- Bewertung des derzeitigen Erfüllungsstands hinsichtlich der NIS-2-Anforderungen
- Erarbeitung notwendiger Maßnahmen gemäß der NIS-2-Richtlinie
- Einblick in Fragen der Haftung, Bußgelder und weiterer Konsequenzen bei Nicht-Erfüllung der Anforderungen
- Hilfestellungen zur Umsetzung der geforderten Sicherheitsmaßnahmen

Sie möchten einen Überblick über das aktuelle Niveau Ihrer IT-Sicherheit erhalten? Mit dem SIEVERS Cyber Security Check (S. 12) überprüfen Sie, wo Sie bereits gut aufgestellt sind – und wo Cyberkriminelle noch leichtes Spiel haben.



SIEVERS Cyber Security Check

Erhalten Sie einen Überblick über das aktuelle Niveau Ihrer IT-Sicherheit: Wie gut sind Sie bereits aufgestellt? Und in welchen Bereichen haben Cyberkriminelle bei Ihnen leichtes Spiel?

Mit dem SIEVERS Cyber Security Check stellen wir Ihre aktuellen IT-Sicherheitsmaßnahmen auf den Prüfstand. Die Ergebnisse des SIEVERS Cyber Security Checks sollen Sie dazu befähigen, die notwendigen Maßnahmen zu definieren und eigenständig umzusetzen. Somit besteht das Ziel des SIEVERS Cyber Security Checks also darin, die IT-Sicherheit Ihrer Organisation zu bewerten und potenzielle Schwachstellen aufzudecken. Diese unabhängige Überprüfung ist entscheidend, um Sicherheitsrisiken zu identifizieren, die von internen Teams möglicherweise übersehen werden. Der Check bietet eine objektive Einsicht in die aktuelle Sicherheitslage und hilft dabei, effektive Maßnahmen zur Risikominimierung zu entwickeln. Durch die Erkennung und Behebung von Sicherheitslücken können Unternehmen ihre Daten und IT-Systeme besser vor Cyberangriffen und Datenlecks schützen. Wir unterstützen Sie auf Ihrem Weg gerne mit Handlungsempfehlungen sowie Best Practices aus unserer Beratungserfahrung.

Ein SIEVERS Cyber Security Check beginnt mit einem eintägigen Workshop bei Ihnen vor Ort. Am Vormittag dieses Workshop-Tages werden alle Teilnehmenden für das Thema Informationssicherheit sensibilisiert, wobei grundlegende Konzepte und Herausforderungen im Bereich der Cybersicherheit vermittelt werden. Am Nachmittag liegt der Fokus auf der Analyse Ihres aktuellen Sicherheitsstatus durch gezielte Fragen, um ein klares Bild der vorhandenen Sicherheitsmaßnahmen und potenziellen Schwachstellen zu erhalten.

Zwei Wochen nach dem Workshop folgt die Ergebnispräsentation, in der wir die identifizierten Schwachstellen besprechen, Maßnahmen zur Verbesserung Ihrer Cybersicherheit priorisieren und konkrete Handlungsempfehlungen geben.

Ihr Nutzen

- **Umfassender Einblick in die IT-Sicherheit:** Bewertung des aktuellen Sicherheitsniveaus und Identifikation von Schwachstellen
- **Maßgeschneiderte Beratung:** Anpassung der Sicherheitsstrategie an die spezifischen Bedürfnisse Ihrer Organisation sowie eine umfassende Beratung zur Auswahl des geeigneten Sicherheitsstandards
- **Zertifizierung und Compliance:** Möglichkeit zur Zertifizierung und Nachweisführung gegenüber Kunden und Geschäftspartnern sowie zur Sicherstellung der Einhaltung relevanter gesetzlicher Anforderungen
- **Eigenständige Sicherheitsverbesserung:** Befähigung zur Implementierung notwendiger Maßnahmen, unterstützt durch Expertenberatung und Best Practices

SIEVERS Information Security Service

Cyberkriminalität, Erpressungstrojaner, IT-Ausfälle – IT-Vorfälle und dadurch bedingte Betriebsunterbrechungen zählen heute zu den wichtigsten geschäftlichen Risiken. Dementsprechend wird die Informationssicherheit zu einem der höchsten Güter – und dabei handelt es sich aufgrund immer neuer und sich stetig ändernder Bedrohungen um einen niemals endenden Prozess, der kontinuierlich verbessert und auf aktuelle Ereignisse abgestimmt werden muss. Ein solcher Prozess wird auch als Informationssicherheitsmanagementsystem (engl.: Information Security Management System, auch: ISMS) bezeichnet.

Für ein erfolgreiches ISMS ist es erforderlich, Informationssicherheit in die DNA des Unternehmens einzubetten, Verantwortlichkeiten festzulegen und den grundsätzlichen Stellenwert des Themas im Unternehmen oder der Organisation zu kommunizieren. Mit unserem SIEVERS Information Security Service helfen wir Ihnen dabei! Gemeinsam mit unseren Profis setzen Sie die ISMS-Implementierung gemäß der VdS 10000-Vorgaben für die organisatorische und technische Absicherung Ihrer IT-Infrastruktur um, stellen entsprechende Maßnahmen sicher und entwickeln die Informationssicherheit in Ihrem Unternehmen kontinuierlich weiter. Folgende Leistungen sind Bestandteil des SIEVERS Information Security Services:

- **Projektmanagement:** Für die Umsetzung der VdS 10000-Vorgaben ist ein effizientes Projektmanagement unabdingbar. Dies stellt sicher, dass das Projekt und seine Teilprojekte angemessen geplant, überwacht und gesteuert werden.
- **Coaching und operative Unterstützung:** Neben der Planung, Steuerung und Überwachung unterstützen wir Sie bei der VdS 10000-Umsetzung auch inhaltlich. Lassen Sie sich z.B. bei der methodischen Durchführung von Risikoanalysen sowie der Vorbereitung von Sensibilisierungsmaßnahmen oder Dokumenten wie Richtlinien und Verfahren unterstützen.
- **Weiterentwicklung:** Nach erfolgreicher Umsetzung ist es erforderlich, das ISMS stetig weiterzuentwickeln. Durch die regelmäßige Abstimmung mit unseren Expert:innen erhalten Sie u.a. Einblicke in neue Cyberbedrohungen sowie Unterstützung beim kontinuierlichen Verbesserungsprozess und tagesaktuellen Themen.

Der SIEVERS Information Security Service beinhaltet monatlich einen individuellen Beratungstermin, der remote oder in Präsenz stattfinden kann. Durch die kontinuierliche Betreuung und Unterstützung wird der Fortschritt der Implementierung der Maßnahmen, die sich aus der VdS 10000-Richtlinie ergeben, sichergestellt und gefördert.

Ihr Nutzen

- Möglichst effektive und effiziente Umsetzung der ISMS-Implementierung
- Kontrolle und Verbesserung der Richtlinien und Verfahren
- Kontinuierliche Betreuung und Unterstützung bei der Weiterentwicklung des ISMS
- Unterstützung bei tagesaktuellen Themen
- Erfahrungswerte aus anderen erfolgreichen Projekten
- Beratung und Begleitung der Verantwortlichen
- Methodische Unterstützung, beispielsweise im Bereich Risikomanagement

SIEVERS SAT (Security Awareness Training)

Die Bedrohung durch Cyberangriffe nimmt für Unternehmen jedweder Branche stetig zu. Dabei genügt es Hackern, sich über das sprichwörtlich „schwächste Glied der Kette“ erfolgreich in Ihr Netzwerk einzuschleusen – und das ist nicht selten der Faktor Mensch. Um die IT-Sicherheit Ihres Unternehmens zu stärken, ist es daher nahezu unabdingbar, Ihre Mitarbeitenden für entsprechende Gefahren zu sensibilisieren und auf die richtigen Handlungswege im Ernstfall vorzubereiten.

Genau hier setzt unser SIEVERS Security Awareness Training (SAT) an: SIEVERS SAT bietet Ihnen praxisnahe Tipps, mit denen Ihre Mitarbeitenden als Einzelpersonen – und dennoch gemeinsam – die Sicherheit Ihres Unternehmens steigern können. Dabei handelt es sich um ein auf Ihr Unternehmen abgestimmtes Training mit individuellen Schwerpunkten. Das SAT wird zielgruppengerecht unter Einbeziehung firmenspezifischer Regelungen und der bereits bestehenden IT-Sicherheitsrichtlinie Ihres Unternehmens von unseren Expert:innen für Ihr Personal vorbereitet und durchgeführt. Der Fokus des Trainings kann u.a. auf folgenden Inhalten liegen:

- Motivation und Verständnis für Informationssicherheit
- Priorität und Kultur der Cybersecurity
- Sicherer Umgang mit dem Internet
- Sichere Benutzung der bereitgestellten Infrastruktur (Laptop, Smartphone, Tablet etc.)
- Erkennung von „schädlichen“ E-Mails
- Sichere Zugangskennungen und Passwörter
- Speicherung und Sicherung von Dateien
- Verhalten bei Sicherheitsvorfällen

SIEVERS SAT kann in Präsenz bei Ihnen im Unternehmen, remote über Microsoft Teams oder in einer hybriden Kombination stattfinden. Darüber hinaus unterstützen wir Sie bei der Vorbereitung der Schulungsinhalte für Ihre interne E-Learning-Plattform.

Ihr Nutzen

- Aktiver Schutz vor Cyberangriffen durch geschulte Mitarbeitende
- Umfangreiches, individuelles und zielgruppengerechtes Trainingsformat
- Praxisnahe Tipps auf Basis Ihrer bestehenden IT-Sicherheitsrichtlinie und unserer Beratungserfahrung
- Langfristiger Ansatz und nachhaltige Konzepte für Ihre Cybersecurity, die auch künftige Onboardings berücksichtigen
- Kombinierbar mit der automatisierten Trainingslösung SIEVERS Security Awareness Service (SAS)

Für einen nachhaltigen Lerneffekt empfehlen wir, SIEVERS SAT mit der technisch automatisierten Schulungslösung SIEVERS SAS (Security Awareness Service, S. 25) zu kombinieren.

SIEVERS Business Continuity Management System (BCMS)

Angesichts von Notfällen oder Krisen ist es für Unternehmen unerlässlich, sicherzustellen, dass geschäftskritische Prozesse so schnell wie möglich wieder anlaufen und so effizient wie möglich in einen Regelbetrieb zurückgeführt werden. Dabei helfen kann ein Business Continuity Management System (BCMS): Hierbei handelt es sich um einen strategischen Ansatz, durch den Schlüsselprozesse proaktiv identifiziert und geschützt, die Reaktionsfähigkeit erhöht, Ausfallzeiten minimiert, das Fortbestehen von geschäftskritischen Prozessen sichergestellt und somit die Resilienz Ihres Unternehmens nachhaltig gestärkt werden.

Unser SIEVERS Business Continuity Management System zielt darauf ab, Ihr Unternehmen auf unerwartete Ereignisse vorzubereiten und die Reaktionsfähigkeit im Falle von Notfällen und Krisenzeiten zu erhöhen. Durch die Analyse Ihrer Geschäftsprozesse erkennen wir kritische Bereiche, die potenzielle Risiken darstellen könnten, und schaffen präventiv individuelle Pläne, um Ausfallzeiten zu verringern und eine schnelle Wiederherstellung geschäftskritischer Prozesse zu gewährleisten.

Dabei konzentrieren wir uns darauf, die kurzfristige Erholungsfähigkeit und langfristige Widerstandskraft Ihres Unternehmens zu fördern: Es werden potenzielle Risiken evaluiert und proaktive Strategien implementiert, die die Geschäftskontinuität selbst in den schwierigsten Zeiten gewährleisten. Eine sorgfältige Bewertung der Geschäftsbereiche, insbesondere der IT-Systeme, ist integraler Bestandteil dieses Ansatzes, um die Betriebssicherheit und Zuverlässigkeit zu erhöhen. Durch eine detaillierte Untersuchung wesentlicher Aspekte Ihrer Geschäftsabläufe werden kritische Bereiche identifiziert, die potenzielle Risiken darstellen könnten. Wir prüfen nicht nur die aktuellen Prozesse, sondern antizipieren auch zukünftige Herausforderungen und sorgen für eine optimierte Prozesssicherheit. Dieser proaktive Ansatz ermöglicht es uns, Notfallpläne zu entwickeln, die genau auf die Bedürfnisse und Anforderungen Ihres Unternehmens zugeschnitten sind. Ein derart maßgeschneiderter Ansatz schafft nicht nur Vertrauen bei Stakeholdern, sondern stärkt auch die Marktposition durch erhöhte Zuverlässigkeit und Glaubwürdigkeit.

Der Service umfasst die Entwicklung und Umsetzung von BCMS-Strategien, das Erstellen und Testen von Notfallplänen und die Unterstützung sowie Schulung von Mitarbeitenden. Mit regelmäßigen Überprüfungen und Updates gewährleisten wir, dass Ihr BCMS stets den aktuellen Herausforderungen gewachsen ist.

Ihr Nutzen

- **Erhöhung der Reaktionsfähigkeit:** Schnellere Reaktion auf unerwartete Ereignisse und Minimierung von Ausfallzeiten
- **Reduzierung der Wiederanlaufzeiten:** Beschleunigter Wiederanlauf geschäftskritischer Prozesse nach einer Störung
- **Effektive Krisenkommunikation:** Sicherstellung einer klaren und zielgerichteten Kommunikation während eines Vorfalls
- Der modernisierte BSI-Standard 200-4 bietet eine praxisnahe Anleitung, um ein Business Continuity Management System in der eigenen Institution aufzubauen und zu etablieren.

Microsoft Security Checks

Das Cybercrime-Geschäft wächst – und mit ihm die Bedeutung von präventiven IT-Sicherheitsmaßnahmen. Setzen Sie auf die Expertise unserer erfahrenen Consultants – im Rahmen unserer MS Security Checks werden nicht nur kritische Sicherheitslagen in Ihrem MS Active Directory, Admin Center, Tenant oder weiteren Office 365-Bereichen aufgedeckt, sondern gleichzeitig auch adäquate Optimierungsansätze in Form von konkreten Handlungsempfehlungen verfolgt.

Darüber hinaus erhalten Sie mit jedem Security Check die SIEVERS-GROUP-Garantie: Sollten wir keine Mängel finden, ist unsere Beratungsleistung für Sie kostenfrei!

Unsere Checks

Microsoft Active Directory Security Check

- Professionelle Beratungsleistung
- Teilautomatisierte Prüfung des lokalen Active Directorys
- Umfangreiche Analysedokumentation
- Detaillierte Sicherheitsbewertung
- Identifizierung von Sicherheitslücken, gefährlicher Standardeinstellungen und fehlerhafter Konfigurationen

Microsoft Tenant Security Check

- Professionelle Beratungsleistung
- Teilautomatisierte Prüfung des Admin Centers mit 85 Prüfpunkten
- Umfangreiche Analysedokumentation
- Detaillierte Sicherheitsbewertung
- Identifizierung von Sicherheitslücken, gefährlicher Standardeinstellungen und fehlerhafter Konfigurationen

Microsoft Tenant Basic Check

- 1-Tages-Workshop mit erfahrenem Microsoft-Consultant
- Best-Practices für den Microsoft Azure Tenant
- Sichtung der Office-365-Umgebung & Tenant-Grundeinstellungen
- Erkennen von Nutzungs- und Optimierungspotenzialen
- Prüfung u.a. von Zugriffs- und Freigaberichtlinien, Teams- und Geräte-Policies, Telemetrie, Analysewerkzeugen, DSGVO und Datenschutzrichtlinien

SIEVERS IT-Compliance Newsletter

Angesichts immer neuer Richtlinien, Gesetze und anderer Entwicklungen im IT-Recht fällt es Ihnen schwer, durch den Informationsdschungel zu navigieren – und die für Ihr Unternehmen relevanten Themen herauszufiltern? Genau hier setzt unser Service im IT-Compliance-Bereich an: Lassen Sie sich ein Mal pro Quartal bedeutende, relevante IT-rechtliche Informationen vorgefiltert, komprimiert und verständlich zusammengefasst per exklusivem Newsletter zustellen – mit unserem SIEVERS IT-Compliance Newsletter!

Was Sie von unserem Newsletter erwarten dürfen? – Stets relevante und praxisorientierte Informationen: Unsere Mitarbeitenden analysieren regelmäßig die aktuellen Entwicklungen im IT-Recht und fassen die Informationen, die für die meisten Unternehmen von Relevanz sind, zusammen. So erhalten Sie vier Mal jährlich eine Übersicht über bedeutende rechtliche Veränderungen, ohne interne Ressourcen für eine aufwendige Recherche und Überwachung binden zu müssen. Dies ermöglicht es Ihnen, Zeit und Ressourcen zu sparen und sich auf Ihr Kerngeschäft zu konzentrieren.

Ihr Nutzen

- Übersichtliche Zusammenfassung bedeutender, relevanter IT-Rechtsentwicklungen
- Relevante und praxisorientierte Informationen
- Effizienzgewinn durch vorgefilterte Informationen
- Kostenoptimierung durch externe Expertise

Managed Security Services (MSS)

SIEVERS Pentesting

Lassen Sie sich von uns hacken – und schützen Sie damit Ihr Unternehmen vor Cyberangriffen – mit unserem professionellen Pentest-as-a-Service. Wieso? Angriffsmethoden organisierter Hacker ändern sich rasant, um bekannte Sicherheitsmaßnahmen zu umgehen und neue Sicherheitslücken auszunutzen. Gleichzeitig unterliegt aber auch Ihre IT-Infrastruktur stetigen Veränderungen. Wie sicher können Sie sich da sein, dass Ihre bisherigen Security-Instrumente vollumfänglich und zu jedem Zeitpunkt ausreichend greifen?

Ein Penetrationstest (kurz: Pentest) ist eine individuelle Sicherheitsüberprüfung, die einen Hackerangriff simuliert. Hierbei werden geprüfte Tools und Mechanismen von sogenannten Pentestern im abgesprochenen Rahmen ausgeführt und validiert. Die Sicherheit Ihrer IT-Infrastruktur wird also verbessert, indem unsere Pentester Schwachstellen und potenzielle Angriffsvektoren identifizieren, bevor Cyberkriminelle diese ausnutzen können. Mögliche Ausprägungen von Penetrationstests sind u.a. Infrastruktur-Tests, Webapplikations-Tests, API-Tests, WLAN-Tests, Phishing-Tests sowie Social-Engineering-Tests. Diese sollten in regelmäßigen Abständen durchgeführt werden, um sicherzustellen, dass die Sicherheitsmaßnahmen des Unternehmens auf dem neuesten Stand sind und potenzielle Schwachstellen schnell identifiziert und behoben werden können. Aber auch nach signifikanten Änderungen an der IT-Infrastruktur oder den Geschäftsprozessen sowie nach Sicherheitsvorfällen sind Pentests sinnvoll. Unsere Expert:innen für Penetrationstests verfügen über eine langjährige Security-Erfahrung und gehen bei ihrer Arbeit gleichermaßen gezielt wie kundenorientiert vor. Die richtige Wahl des möglichen Angriffsszenarios ist entscheidend – die Schwachstellenidentifikation sollte nicht erst durch reale Angriffe entstehen. Um herauszufinden, wo genau in Ihrer IT-Infrastruktur potenzielle Sicherheitslücken Hackern Tür und Tor öffnen, und diesen entgegenzuwirken, bieten wir Ihnen im Rahmen unseres Pentest-Services gleich zwei verschiedene Pentesting-Optionen an: den Project Pentest und den Pentest-as-a-Service (PtaaS).

- **Project Pentest:** Mit dem Project Pentest führen wir einmalig eine umfassende Untersuchung Ihrer IT-Systeme durch, um Schwachstellen zu identifizieren und zu bewerten. Dabei arbeiten wir eng mit Ihnen zusammen und stellen sicher, dass wir alle Ihre Anforderungen und Bedenken berücksichtigen. Am Ende des Projekts erhalten Sie einen detaillierten Bericht mit unseren Ergebnissen und weiterführenden Handlungsempfehlungen.

- **Pentest-as-a-Service:** Alternativ können Sie sich für unseren Pentest-as-a-Service (PtaaS) entscheiden. Hierbei handelt es sich um einen kontinuierlichen Service, bei dem wir regelmäßige Pentests durchführen, um potenzielle Schwachstellen zu identifizieren und zu bewerten. Diese Option bietet Ihnen eine fortlaufende Überwachung Ihrer IT-Sicherheit und ermöglicht es Ihnen, neue Bedrohungen zu erkennen und auf diese effizient zu reagieren.

Die SIEVERS-GROUP zeichnet sich als Pentest-Anbieter durch einen ganzheitlichen Service aus. Im Gegensatz zu vielen Anbietern, die nach einem Pentest lediglich Handlungsempfehlungen aussprechen, bieten wir darüber hinaus aktive Unterstützung bei der Umsetzung dieser Maßnahmen. Unser Team aus erfahrenen IT-Sicherheitsexpert:innen engagiert sich täglich für die Sicherheit und den Erfolg unserer Kunden. Wir entwickeln maßgeschneiderte Lösungen, um die IT-Infrastruktur unserer Partner effektiv zu schützen. Dieser Ansatz garantiert nicht nur eine umfassende Aufklärung über Sicherheitsrisiken, sondern auch die Bereitstellung praktischer und individuell angepasster Lösungen zur Stärkung Ihrer IT-Sicherheit.

Ihr Nutzen

- Frühzeitiges Erkennen und Schließen von Schwachstellen
- Risikoarme Überprüfung
- Überblick über Ihre IT-Sicherheitslage
- Entscheidungshilfe zum Ausbau der IT-Sicherheitsstrategie
- Praxis- und realitätsnahes Aufzeigen von Hackerarbeit
- Verhinderung von Ernstfällen
- Wirksamkeitsüberprüfung der bereits vorhandenen IT-Sicherheit
- Unterstützung bei der Einhaltung von Regularien und der Vorbereitung auf Security-Audits

SIEVERS MailSec

E-Mails sind nach wie vor der führende Bedrohungsfaktor für Ransomware, Phishing, Datendiebstahl und andere raffiniert ausgeklügelte Cyberattacken – Unternehmen können es sich deshalb nicht leisten, an diesem sensiblen Punkt ungeschützt zu bleiben. Mit der E-Mail-Security-Lösung SIEVERS MailSec erhalten Sie eine übergreifende Lösung mit vielseitigen Features, die den Schutz Ihrer E-Mail- und Datensicherheit gewährleisten.

Ihr Nutzen

- Filterung von ein- und ausgehenden E-Mails
- Filterung schädlicher Inhalte (z.B. Viren)
- Filterung unerwünschter Werbung (z.B. Spam)
- Filterung legitimer Werbung (z.B. Newsletter)
- White- und Blacklist-Funktionen
- Content- und Compliance-Filterung
- Spam-Erkennungsrate von mindestens 99,9 %

SIEVERS MailSec 365

Mit der zunehmenden Verlagerung von Mail-Servern in die Cloud (insbesondere Exchange Online) steigt auch das Anforderungsprofil an entsprechende Security-Lösungen. Auch bei der cloudbasierten Nutzung von Microsoft 365-Produkten empfiehlt es sich, eine weitere Sicherheitsebene zu implementieren. Schließlich meldet Hersteller Microsoft immer wieder einen Anstieg an gezielten Angriffen auf Microsoft 365-Konten. Die Lösung der SIEVERS-GROUP: SIEVERS MailSec 365! Der cloudbasierte All-in-one-Security- und Backup-Service ist die Antwort auf die komplexen, neuen Herausforderungen – und sichert Ihr Unternehmen in puncto Security, Compliance und Backup ideal ab. SIEVERS MailSec 365 schützt Ihren Microsoft 365-Tenant vollumfänglich vor Phishing, Ransomware und Advanced Persistent Threats – und bewahrt Sie vor dem damit leider viel zu oft verbundenen Verlust sensibler Daten und Informationen.

Ihr Nutzen

- Spam & Malware Protection
- E-Mail Encryption
- E-Mail Signatures & Disclaimers
- Advanced Threat Protection
- E-Mail-Archivierung
- E-Mail-Continuity
- Backup & Recovery of Mailboxes & Teams
- Backup & Recovery of SharePoint & OneDrive
- Priorisierter Service & Support durch die SIEVERS-GROUP
- Höchste Spam- und Malware-Erkennungsraten am Markt
- KI-basierte Filtermechanismen zur Identifizierung komplexer Angriffe
- Automatisierte Backups mehrmals täglich – einmal einrichten und fertig
- Schutz von Dateien auf Ihren Endpoints
- Administration in einem zentralen Control-Panel

	SIEVERS MailSec	SIEVERS MailSec 365
SIEVERS-GROUP Service Desk	✓	✓
Alarmierung bei Störungen	automatisch zum Service Desk (SIEVERS-GROUP)	
Intervention bei Störungen des E-Mail-Verkehrs	✓	✓
Abrechnungsmodell	je Postfach	je M365 Cloud-Lizenz*
Geteiltes Administrationsmodell	✓	✓
Rechenzentrumsstandort	✓	✓
Pflege kundenspezifischer Freigabelisten	automatisch zum Service Desk (SIEVERS-GROUP)	
E-Mail-Quarantäne-Verwaltung (Freigabe/Blockierung)	automatisch zum Service Desk (SIEVERS-GROUP)	
Spam- und Virenfilter für eingehende/ausgehende E-Mails	✓	✓
Content- und Compliance-Filter	✓	✓
Transportwegverschlüsselung (TLS)	✓	✓
Schutz vor gezielten und komplexen Angriffsmustern	✓	✓
Prüfung, Ausführung und Analyse verdächtiger Anhänge in einer sicheren Umgebung (ATP, Sandboxing)	✓	✓
Verhaltensanalyse von verdächtigen Link-Zielen	✓	✓
Plausibilitätsprüfung von Absender- und Metadaten	✓	✓
Analyse von verschlüsselten Office- und PDF-Dateien	✓	✓
E-Mail-Signatur & Company Disclaimer	optional	✓
Automatische, richtlinienbasierte E-Mail-Verschlüsselung	optional	✓
E-Mail-Archivierung für bis zu 10 Jahre	optional	✓
E-Mail-Backup für 90 Tage bei Mailserver-Ausfall	optional	✓
Backup & Recovery für Microsoft 365-Applikationen	/	optional

* mit akt. Exchange Feature

Zusatzoptionen für noch mehr Sicherheit

- Datensicherung und Wiederherstellung für Microsoft 365-Applikationen (nur für Paket: MailSec 365)
- Verschlüsselung des E-Mail-Verkehrs (nur für Paket: MailSec 365)
- E-Mail-Archivierung / Vorhaltezeitraum: 10 Jahre inkl. 25 GB Speichervolumen über alle Postfächer gemittelt (nur für Paket: MailSec 365)
- Signatur & Disclaimer (nur für Paket: MailSec 365)
- Hosting und Verwaltung der Domain auf redundant gesicherten DNS-Servern

SIEVERS Endpoint Protection

IT-Verantwortliche stehen vor der Herausforderung, Systeme kontinuierlich vor einer Vielzahl von Bedrohungen zu schützen. SIEVERS Endpoint Protection wurde genau dafür entwickelt – um einen umfassenden, zuverlässigen Schutz für Clients und Server zu bieten, der sich nahtlos in bestehende Infrastrukturen integrieren lässt. Mit unseren erstklassigen Sicherheitslösungen sind Sie optimal vorbereitet.

Die SIEVERS Endpoint Protection-Lösung ist so konzipiert, dass sie den spezifischen Anforderungen einer breiten Palette von IT-Infrastrukturen gerecht wird: Sei es in Cloud-Umgebungen, auf lokalen Servern oder in hybriden Setups – der Endpoint Protection Service kann flexibel angepasst und integriert werden. Der nahtlose Einbezug unseres Service in existierende Systeme ermöglicht eine effiziente und unkomplizierte Implementierung, sodass Unternehmen ihre Ressourcen und Zeit für ihre Kerngeschäftsaktivitäten nutzen können. Dank der umfassenden Integrationskapazität erweist sich unser Service darüber hinaus als besonders wertvoll für mittelständische Unternehmen, die oft mit heterogenen und vielseitigen IT-Landschaften arbeiten, und findet branchenübergreifend Anwendungsgebiete:

- **Dienstleistungssektor:** Unser Service verstärkt die Sicherheitsstandards und minimiert Risiken, die durch den Umgang mit Kundendaten und Kommunikation entstehen können.
- **Gesundheitswesen:** Der Schutz von Patientendaten und der sichere Betrieb von medizinischen Geräten sind essenziell. Hierbei erhöht der Endpoint Protection Service die Sicherheitsmaßnahmen.
- **Produktion und Industrie:** Die Anzahl vernetzter Systeme steigt stetig an. Auch hierbei unterstützt unser Service Unternehmen, um ihre Sicherheitsprotokolle zu stärken und besser auf mögliche Bedrohungen vorbereitet zu sein.
- **Bildung:** Schulen, Universitäten und andere Bildungseinrichtungen, die immer mehr auf digitale Technologien setzen, können mit unserem Service die Resilienz gegenüber Cyberbedrohungen verbessern und das digitale Lernumfeld absichern.
- **Freizeit und Tourismus:** Online-Interaktionen – von der Buchung bis zur Kundenbewertung – sind zentral in diesem Sektor. Unser Service optimiert die Schutzmechanismen für Kundendaten und Online-Plattformen.

Ihr Nutzen

- Schutz Ihrer Server vor den neuesten Cyberbedrohungen
- Verhaltensbasierte Erkennung von Bedrohungen
- Schutz vor Ransomware
- Kontinuierliche Überwachung
- Zusätzliche Kontrollfunktionen für Ihre Server, File Integrity Monitoring, Application-Whitelisting und detaillierte Einblicke in die Cloud-Umgebung Ihres Unternehmens
- Anpassungsfähigkeit an diverse Infrastrukturen
- Nahtlose Integration in bestehende Systeme
- Transparenz durch unser flexibles, User- und Servergenaues, monatliches Abrechnungsmodell
- Zeitersparnis durch Outsourcing der Endpoint Security (Endpoint-Überwachung) und der Bedrohungsanalyse an die SIEVERS-GROUP
- Ursachenanalyse zur Rekonstruktion erfolgter Angriffe
- Keine Bereitstellung und keine Kosten für eine eigene Infrastruktur

SIEVERS VMS (Vulnerability Management Service)

Die fortschreitende Digitalisierung bringt immense Chancen für den Mittelstand hervor, zieht jedoch gleichzeitig Herausforderungen in der IT-Sicherheit nach sich. Für IT-Verantwortliche steht daher die Frage im Raum: Wie lässt sich eine wachsende IT-Infrastruktur effizient und sicher verwalten? Unser Schwachstellenmanagement-Service SIEVERS VMS bietet hierfür eine zuverlässige Lösung. Entwickelt mit Fokus auf dem deutschen Mittelstand soll diese Lösung Unternehmen nicht nur schützen, sondern ihnen auch ein fundiertes Sicherheitsmanagement an die Hand geben. Die digitale Umgebung ändert sich rasant und mit ihr die Sicherheitsrisiken. Unser Service sorgt dafür, dass IT-Verantwortliche stets einen klaren Überblick über die eigene IT-Landschaft haben. Dies ermöglicht eine proaktive Reaktion auf potenzielle Risiken, anstatt nur auf entstandene Probleme zu reagieren. Für IT-Verantwortliche bietet unser Schwachstellenmanagement-Service somit eine solide Grundlage, um die IT-Sicherheit des Unternehmens kontinuierlich zu stärken und zukunftsorientiert aufzustellen.

Unsere Herangehensweise fokussiert sich auf das Erkennen und Beheben von Schwachstellen, bevor sie zu einem Problem werden. Dies geschieht durch den Einsatz modernster Technologien und Expertise in der IT-Sicherheit. Für Unternehmen bedeutet das eine signifikante Reduzierung von Risiken und die Möglichkeit, sich auf das Kerngeschäft zu konzentrieren.

Sicherheit ist bei uns kein Nebenprodukt, sondern eine Kernkompetenz. Mit uns als Partner an Ihrer Seite sind Sie bestens für die digitalen Herausforderungen von morgen gerüstet.

Ihr Nutzen

- **Präzise Automatisierung:** Ihre IT-Systeme werden durch unsere fortschrittlichen Algorithmen präzise analysiert. Das Ziel: keine Schwachstelle unentdeckt lassen. Eine effektive Erkennung ist der Schlüssel zur Sicherheit.
- **Erfahrung und Innovation im Einklang:** Unsere Expert:innen verknüpfen bewährtes Know-how mit aktuellen technologischen Entwicklungen.
- **Klare und verständliche Berichte:** Dank detaillierter Reports erhalten Sie einen umfassenden Überblick über den Zustand Ihrer IT-Infrastruktur. Jeder Bericht wird durch zielführende Handlungsempfehlungen ergänzt, damit Sie wissen, welche Schritte als nächstes zu unternehmen sind.
- **Individuell angepasste Sicherheitslösungen:** Jedes Unternehmen hat individuelle Sicherheitsbedürfnisse. Deshalb entwickeln wir Strategien, die genau auf Ihr Unternehmen zugeschnitten sind und so den bestmöglichen Schutz bieten.
- **Tiefgehende Sicherheitsanalysen:** Mittels umfangreicher Analysen untersuchen wir Ihr System bis ins kleinste Detail, um Schwachstellen zu identifizieren.
- **Proaktive Risikoerkennung:** Anstatt lediglich auf auftretende Probleme zu reagieren, fokussieren wir uns darauf, potenzielle Risiken frühzeitig zu identifizieren.
- **Ständige Systemoptimierung:** Die IT-Welt befindet sich in einem ständigen Wandel. Daher überprüfen und aktualisieren wir regelmäßig unsere Sicherheitsmaßnahmen, sodass Ihre Systeme stets optimal geschützt sind.

SIEVERS FireSec

Die Anzahl und Komplexität moderner Cyberangriffe steigen seit Jahren exponentiell. Diese Bedrohungslage setzt den Einsatz geeigneter Firewall-Systeme und deren dauerhafte Überwachung und Optimierung voraus – schließlich bilden Firewalls die Basis einer umfassenden IT-Security-Strategie, um Ihre Infrastruktur angemessen vor Cyberattacken zu schützen. Die Evaluierung angemessener Systeme sowie die Bereitstellung personeller und zeitlicher Ressourcen für die nachhaltige Sicherstellung eines optimalen Schutzgrades stellen viele Unternehmen dabei allerdings vor große Herausforderungen:

- Hohe Komplexität des Themas
- Täglich neu auftretende Bedrohungsarten
- Qualifiziertes Personal finden, das sich dieser Themen annimmt

SIEVERS FireSec nimmt Ihnen diese Arbeit ab: Beginnend bei der Auswahl und Konzeptionierung der eingesetzten Hardware kümmern wir uns darüber hinaus um das Monitoring und die regelmäßige Wartung Ihrer Systeme.

Jahrelange Erfahrung und auf Netzwerksicherheit spezialisierte Techniker:innen ermöglichen es uns, Ihnen mit diesem Service ein professionelles Firewall-Management anzubieten. Ihr Firewall-System wird auf die Monitoring-Umgebung unseres Service Desk aufgeschaltet und aktiv überwacht. Dies erlaubt es uns, schnell auf Anomalien an Ihrem Netzwerkperimeter zu reagieren, um einen reibungslosen Betrieb Ihres Unternehmens zu gewährleisten. Unser Service Desk steht Ihnen dabei für Änderungswünsche und Supportanfragen gerne zur Verfügung.

Um den vielfältigen Anforderungen verschiedener Unternehmensgrößen und -strukturen gerecht zu werden, haben wir eine Auswahl an Managed-Firewall-Servicepaketen entwickelt, die speziell darauf abgestimmt sind, unterschiedliche Sicherheitsbedürfnisse zu erfüllen:

- **Basic-Paket:** Dieses Paket bietet grundlegenden Schutz und ist ideal für kleinere Netzwerke geeignet. Es umfasst alle wesentlichen Sicherheitsfunktionen, die erforderlich sind, um ein solides Sicherheitsfundament zu schaffen.
- **Professional-Paket:** Für mittlere bis große Netzwerke mit höheren Sicherheitsanforderungen ist das Professional-Paket konzipiert. Es erweitert den grundlegenden Schutz um zusätzliche Funktionen und bietet eine verstärkte Sicherheitsebene, die auf komplexere Netzwerkstrukturen abgestimmt ist.
- **Enterprise-Paket:** Unternehmen mit umfangreichen und komplexen Netzwerkinfrastrukturen profitieren von unserem Enterprise-Paket. Dieses Paket bietet das höchste Sicherheitsniveau mit fortschrittlichen Lösungen, die speziell für die anspruchsvollsten Sicherheitsanforderungen entwickelt wurden.

Ihr Nutzen

- Gemanagter Firewall-Service für Ihre Infrastruktur
- Überwachung und Administration Ihrer Firewall-Systeme durch unsere Security-Expert:innen
- Kurze Reaktionszeiten bei auftretenden Störungen oder akuten Bedrohungen
- Schnelle und professionelle Hilfe durch unseren Service Desk (Remote-Support)
- Immer auf dem neuesten Stand der Technologie zur Abwehr von Bedrohungen
- Nachhaltige Optimierung Ihrer Firewall-Richtlinien und -Konfiguration
- Durch unsere Finanzierungsmodelle sparen Sie sich hohe Investitionskosten
- Beliebig skalierbar – von KMU bis Distributed Enterprise
- Flexible Vertragslaufzeiten
- Zeitersparnis und planbare Kosten

SIEVERS SAS (Security Awareness Service)

Die Anzahl und Qualität von Cyberangriffen steigt. Die Digitalisierung – und hier vor allem die KI – verschärft die Bedrohungslage, die insbesondere durch Phishing und Ransomware-Attacken gekennzeichnet ist: 95 % aller Hackerangriffe erfolgen per E-Mail! 9 von 10 erfolgreichen Cyberangriffen starten mit einer Phishing-Mail – und getäuschten Mitarbeitenden …

Der Faktor Mensch spielt damit eine wesentliche Rolle für die IT-Sicherheit Ihres Unternehmens. Oder anders ausgedrückt: Wachsames und aufmerksames Handeln muss für alle im Unternehmen zur absoluten Selbstverständlichkeit werden!

Doch wie können Sie Ihre Mitarbeitenden für dieses wichtige Thema und die damit verbundenen digitalen Gefahren sensibilisieren? Die Antwort ist einfach: mit dem SIEVERS SAS.

Der SIEVERS SAS ist ein fortlaufender Software-gestützter Service mit dem Schwerpunkt E-Mail-Security, der auf der Softwarelösung des deutschen Cloud-Security-Providers Hornetsecurity basiert. Im Fokus dieser Lösung steht, eine nachhaltige Sicherheitskultur zu etablieren: Dank realistischer Spear-Phishing-Simulationen und KI-gestütztem E-Training wird das Bewusstsein für Cybersicherheitsrisiken und -bedrohungen bei Ihren Mitarbeitenden geschärft. Damit versetzt der Service Ihre Mitarbeitenden in die Lage, im Ernstfall instinktiv die richtige Entscheidung zu treffen. Die weiteren Pluspunkte: SIEVERS SAS zeichnet sich durch eine einfache Implementierung und nur minimalen Administrationsaufwand aus; so müssen von Ihnen beispielsweise keine Inhalte für Prüfungs-E-Mails vorbereitet werden. Zudem erhalten Sie kontinuierlich Kennzahlen, die Ihnen einen umfassenden Überblick über das aktuelle Sicherheitsniveau geben.

Ihr Nutzen

- Intelligentes Awareness Benchmarking
- Bedarfsgerechte Bereitstellung relevanter E-Trainingsinhalte
- Booster-Option für User, die ein intensiveres E-Training benötigen
- Vollständig automatisierte Steuerung des E-Trainings
- Echtzeit-Monitoring aller Statistiken zum Security Awareness Training
- ESI®-Reporting mit bisherigem ESI®-Verlauf und Forecast
- Konfiguration und Anpassung des Awareness Trainings an die Bedürfnisse Ihres Unternehmens
- User Panel mit zentralem Zugriff auf alle E-Learning-Inhalte
- Auswertung der individuellen Phishing-Simulation eines jeden Users
- Gamification-Ansatz spornt User an, „ihr Bestes zu geben“
- Lerninhalte in mehreren Sprachen verfügbar
- Minimaler Administrationsaufwand

Unser Tipp: Kombinieren Sie!
Für einen nachhaltigen Lerneffekt empfehlen wir, die automatisierte Schulungslösung SIEVERS SAS mit dem Grundlagen-Training SIEVERS SAT (S. 14) zu kombinieren. Mit dieser Security-Awareness-Kombi schaffen Sie in Ihrem Unternehmen das notwendige Bewusstsein für aktuelle IT-Sicherheitsthemen auf allen Ebenen.

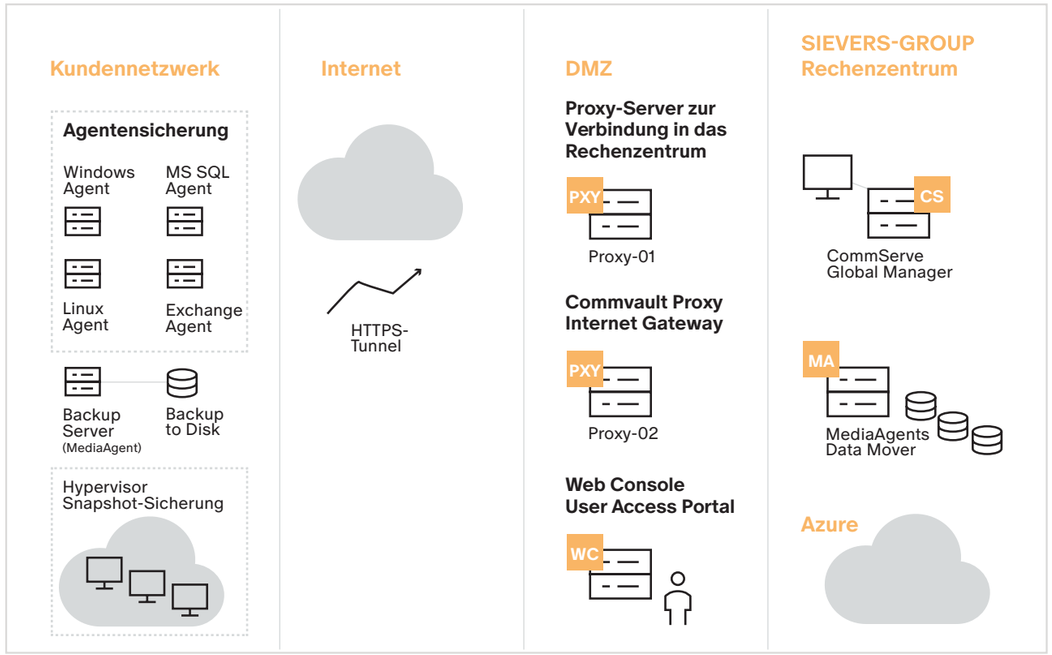
SIEVERS Backup

Die eigenen Datenbestände zählen für viele Unternehmen zu den zentralen Produktionsfaktoren. Daher ist es wichtig, sich mit Backup-Prozessen zu beschäftigen. In der Praxis gilt die Datensicherung im Unternehmen jedoch als wenig bis gar nicht wertschöpfend und wird daher häufig vernachlässigt. Zudem ist es für viele Unternehmen zeitlich gar nicht mehr möglich, sich in aller Tiefe mit Backup-Prozessen zu befassen. Jedoch sollte die Datensicherung im Unternehmen ein zentraler Baustein der IT-Strategie sein.

Profitieren Sie vom SIEVERS Backup: Unsere Backup-Spezialist:innen übernehmen sicher und transparent die Aufgaben der Datenspeicherung und senken so das Risiko von Datenverlusten oder Umsatzausfällen. Eine zentrale Rolle für mehr Sicherheit und Kosteneffizienz spielen hierbei Managed Services: Die SIEVERS-GROUP stellt mit dem SIEVERS Backup standardisierte und bewährte Backup-Lösungen zur Verfügung, um die Anforderungen an eine moderne Datensicherung im Unternehmen zu erfüllen, ohne hohe Investitionen tätigen zu müssen.

Bei dem SIEVERS Backup kommt die bewährte 3-2-1-Regel zum Einsatz, die besagt, dass von den zu schützenden Daten 3 Kopien erstellt, diese Kopien auf 2 verschiedenen Arten von Speichermedien gespeichert und 1 Kopie der Daten an einem externen Speicherort abgelegt werden sollen.

SIEVERS Backup stellt sich in der Funktionsübersicht wie folgt dar:

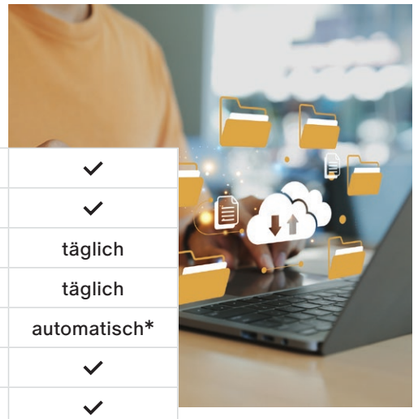


Kundennetzwerk: Die Netzwerksicherung ist ein wesentlicher Bestandteil des Sicherungs- und Wiederherstellungsprozesses in Ihrer IT-Umgebung. Mit unserer Backup-Lösung werden die zu sichernden Netzwerkkomponenten identifiziert, ein Sicherungszeitplan konfiguriert und die Daten in einen Sicherungsspeicher kopiert.

Internet: Mittels HTTPS-Tunnel wird eine Netzwerkverbindung zwischen den Endgeräten hergestellt. Der Tunnel wird von einem Vermittler, dem Proxy-Server, erstellt. Dieser befindet sich normalerweise in einer DMZ.
DMZ: Ziel des DMZ-Netzwerks ist es, das lokale Netzwerk Ihres Unternehmens zusätzlich zu schützen. Ein geschützter und gut überwachter Netzwerkknoten, der sich außerhalb des internen Netzwerks befindet, kann auf die Dienste zugreifen, die in der DMZ verfügbar sind, während der Rest des Unternehmensnetzwerks durch eine Firewall gesichert wird.
SIEVERS-GROUP-Rechenzentrum: Eine Kopie Ihrer Daten wird in dem von der SIEVERS-GROUP betriebenen Rechenzentrum in Düsseldorf gesichert.
Azure: Optional kann eine Datensicherung auf der Cloud-Plattform Microsoft Azure erfolgen.

Ihr Nutzen

- Initiale Sicherung in der Kundenumgebung
- Kopie in das SIEVERS-GROUP-RZ Düsseldorf
- Kopie in den SIEVERS-GROUP-Azure-Tenant
- 256-Bit-AES-Verschlüsselung
- Proxy-basierte Umgebung
- Schutz vor Ransomware/unbefugtem Löschen
- Wiederherstellung von VMs oder Dateien an ursprünglicher Stelle
- Cross-Hypervisor Restore
- Replikation
- Azure to Azure (Subscription- und regionsunabhängig)
- On-Prem Hypervisor zu Azure
- Managed Services
- Backup-Kopie an einem externen Speicherort
- Moderne Datensicherung ohne hohe Investitionen



Serviceübersicht: SIEVERS Backup

SIEVERS-GROUP Service Desk	✓
Vielfältige Sicherungsagenten für alle gängigen Plattformen	✓
Intervall der Datensicherungen	täglich
Monitoring der Datensicherungen	täglich
Alarmierung bei Backup-Fehlern	automatisch*
Proaktive Intervention bei Backup-Fehlern	✓
Geteilter Zugriff auf Service-Plattform	✓
Self-Service Restore via Backup-Portal	✓
Aufbewahrungszeit der Datensicherungen	✓
Proaktive Aktualisierung der Softwarekomponenten	✓
Verschlüsselte Datenübertragung	✓
Georedundante Datenhaltung	✓
Datenverarbeitung in zertifizierten Rechenzentren innerhalb der EU	✓
Lizenzverwaltung	✓
ISO 27001-zertifizierte SIEVERS-GROUP-Enterprise Cloud	✓

** zum Service Desk der SIEVERS-GROUP*

SIEVERS Backup M365

Microsoft 365 dient Millionen Business-Kunden als zentrale Produktivitätsplattform, über die sensible Daten ausgetauscht werden. Sollte es jedoch durch Systemausfälle oder Cyberangriffe zum Verlust wichtiger Unternehmensinformationen kommen, bietet Microsoft keine nativen Optionen zur Sicherung und Wiederherstellung. Mit dem SIEVERS Backup M365 für Microsoft profitieren Sie von einer umfassenden Backup- und Recovery-Lösung für Microsoft 365-Postfächer, Teams-Chats, OneDrive für Business-Konten, SharePoint-Dokumentenbibliotheken und vieles mehr. Dank der einfachen Konfiguration können wir Ihre Microsoft 365-Daten problemlos sichern, verwalten und wiederherstellen. Schützen Sie Ihre Microsoft-Services durch das SIEVERS Backup M365:

- **Exchange:** Datensicherung Ihrer Outlook-Mailboxen, Archive, Ordner, Chats, Kalender, Kontakte, Nachrichten, Berechtigungen und mehr
- **OneDrive:** Datensicherung Ihrer Listen, Bibliotheken, Ordner, Elemente, Metadaten, Sicherheitseinstellungen und Versionsverläufe in OneDrive
- **SharePoint:** Schutz Ihrer Site Collections oder granularer Sites, Listen, Bibliotheken, Ordner, Elemente, Metadaten, Sicherheitseinstellungen und Versionsverläufe
- **Project:** Datensicherung Ihrer Pläne, Aufträge, Aufgaben und Dateien in Project
- **Yammer:** Schutz Ihrer Beiträge, Dokumente, Umfragen, Gruppen und mehr
- **Teams:** Datensicherung Ihrer Teams-Kanäle, privater Kanäle, Konversationen, Arbeitsdateien, Besprechungselemente und mehr
- **Öffentliche Ordner:** Schutz Ihrer Mailboxen, Nachrichten, Dateien, Kontakte, Formulare und Postings

Ihr Nutzen

- Sicherung Ihrer Microsoft 365-Apps
- Monitoring der Datensicherungen
- Unlimitierte Datenmenge
- Bis zu 4 Sicherungen pro Tag
- Unlimitierte Vorhaltezeit der Daten

IS4IT Incident Response Management

Cybercrime ist dynamisch: In der heutigen digitalen Welt sind Unternehmen und Organisationen ständig wachsenden Bedrohungen ausgesetzt. Cyberangriffe, Datenlecks und Systemausfälle können dabei enorme Schäden anrichten – sowohl finanziell als auch in Bezug auf das Vertrauen der Kunden. Eine schnelle und effektive Reaktion auf Sicherheitsvorfälle ist daher unerlässlich. Hier kommt das Incident Response Management ins Spiel.

Incident Response ist eine moderne Security-Strategie, die Unternehmen dabei hilft, konsequent und umfassend auf IT-Sicherheitsvorfälle zu reagieren und sie zu bewältigen. Ziel ist es, die Auswirkungen eines Vorfalls zu minimieren, schnell wieder zur Normalität zurückzukehren und zukünftige Angriffe zu verhindern. Ein gut vorbereitetes Incident Response Team kann den Unterschied zwischen einem kleinen Zwischenfall und einem in großem Stil durchgeführten, komplexen Cyberangriff ausmachen, der aus einem umfangreichen Diebstahl sensibler Daten oder einer weitreichenden digitalen Sabotage von Systemen besteht.

Unser Incident-Response-Ansatz basiert auf einem bewährten und strukturierten Prozess, der sich in mehrere Phasen gliedert:

- **Vorbereitung:** Identifizierung von Risiken, Schulung des Teams und Entwicklung eines Incident-Response-Plans
- **Erkennung und Analyse:** Schnelles Erkennen eines Vorfalls, gefolgt von einer detaillierten Analyse zur Bestimmung des Ausmaßes und der Ursache
- **Eindämmung:** Maßnahmen zur Begrenzung der Auswirkungen und zur Verhinderung einer weiteren Ausbreitung des Vorfalls
- **Beseitigung:** Identifizierung und Entfernung der Bedrohung aus den betroffenen Systemen
- **Wiederherstellung:** Sicherstellen, dass die Systeme wieder ordnungsgemäß in Betrieb genommen werden können
- **Nachbereitung:** Analyse des Vorfalls zur Verbesserung zukünftiger Reaktionen, Aktualisierung der Sicherheitsmaßnahmen und weitere Schulung des Teams

In Zusammenarbeit mit unserem strategischen Partner IS4IT bieten wir maßgeschneiderte Incident Response Services, die genau auf die Bedürfnisse Ihres Unternehmens abgestimmt sind. Im Security Operations Center der IS4IT in Oberhaching überwachen rd. 40 erfahrene Security-Spezialisten 24/7 an 365 Tagen im Jahr die IT-Netzwerke und -Systeme von Kunden. Das „Computer Security Incident Response Team“ (CSIRT) von IS4IT verfügt neben einer erstklassigen IT-Sicherheitsmannschaft auch über erfahrene Expert:innen für Täterkommunikation und Verhandlungen sowie Krisenmanagement und -kommunikation. Die Zusammenarbeit mit den Strafverfolgungsbehörden und dem BSI sowie Spezialisten für klassische Ermittlungen ist ein eingeübter Prozess: Das CSIRT hat in den vergangenen Jahren mehr als 50 Fälle von Industriespionage und Ransomware bearbeitet, die nur durch umfangreiches Know-how und langjährige Erfahrung erfolgreich abgeschlossen werden konnten. IS4IT gilt deshalb bundesweit als Experte für die Vorfallsbearbeitung.

Ihr Nutzen

- **Minimierung von Schäden:** Eine schnelle Reaktion kann den potenziellen Schaden eines Sicherheitsvorfalls erheblich reduzieren.
- **Wiederherstellung des Betriebs:** Durch systematische Schritte wird die Wiederherstellung der normalen Betriebsabläufe beschleunigt.
- **Schutz von Daten:** Mit einem klaren Plan können Datenverluste minimiert oder verhindert werden.
- **Vertrauensschutz:** Ein transparenter und effektiver Umgang mit Vorfällen stärkt das Vertrauen der Kunden und Partner.
- **Rechtliche und regulatorische Einhaltung:** Incident Response hilft Ihnen, gesetzliche Anforderungen zu erfüllen und hohe Bußgelder zu vermeiden.

IS4IT SOC

Ein SOC (Security Operations Center) ist ein Dienst für externe Sicherheitsüberwachung und -management. Es handelt sich um ein Team von Expert:innen, das Sicherheitsvorfälle rund um die Uhr überwacht, analysiert und darauf reagiert. Gerade hinsichtlich der stetig wachsenden Zahl an Cyberbedrohungen sind eine durchdachte Sicherheitsstrategie sowie kontinuierliche Überwachung der IT-Infrastruktur mittlerweile unerlässlich. Ein Managed Security Operations Center (Managed SOC) ist darauf ausgelegt, die komplexen Sicherheitsbedürfnisse moderner Unternehmen zu erfüllen und eine fortlaufende Absicherung kritischer IT-Systeme sicherzustellen.

Mit dem Managed SOC bieten wir Ihnen eine umfassende Cybersicherheit und Überwachung zu kontrollierbaren Kosten. Dies geschieht, indem wir eine individuell angepasste Überwachungs- und Analysestrategie anwenden, die auf den jeweiligen Sicherheitsanforderungen des Unternehmens basiert und durch die Verwendung von fortschrittlichen SIEM-, SOAR- und NDR-Technologien realisiert wird. Dadurch können wir Ihnen einen umfassenden Schutz bieten. Zu den Dienstleistungen gehören in der Regel 24/7-Überwachung, Incident Response, Bedrohungsanalyse und -intelligenz, Log-Management, Compliance-Management und regelmäßige Berichterstattung. Unsere Expert:innen überwachen kontinuierlich die IT-Infrastruktur und stellen so sicher, dass alle Systeme optimal geschützt sind, während gleichzeitig die Betriebskosten dank eines hohen Maßes an standardisierten und automatisierten Abläufen überschaubar und planbar bleiben. Im Falle eines Sicherheitsvorfalls informiert das SOC Sie gemäß vorher festgelegter Protokolle; dies kann über automatisierte Alerts, E-Mails oder Telefonanrufe erfolgen. Die Datensicherheit wird durch den Einsatz von Verschlüsselung, sicheren VPNs und strengen Zugriffskontrollen gewährleistet. Zudem werden Datenschutzvereinbarungen und Compliance mit relevanten Standards, wie ISO 27001 oder dem Grundschutz des Bundesamts für Sicherheit in der Informationstechnik, berücksichtigt. Die Qualitätssicherung erfolgt durch regelmäßige Audits, die Einhaltung von Service Level Agreements (SLAs), kontinuierliche Fortbildung des Personals und Anpassungen der Dienste an sich ändernde Bedrohungsszenarien.

Die Integration erfolgt durch die Einrichtung sicherer Log- und Datenkanäle zwischen der IT-Infrastruktur Ihres Unternehmens und dem SOC. Die Implementierungszeit variiert dabei je nach Komplexität der IT-Infrastruktur und der erforderlichen Integration. Im Allgemeinen kann ein grundlegendes Setup in wenigen Wochen realisiert werden. Je nach individuellem Bedarf bieten wir Ihnen unterschiedliche Service-Levels und Leistungspakete, die sich nach dem Umfang der Dienstleistungen, der gewünschten Reaktionszeit bei Vorfällen und der Tiefe der Berichterstattung berechnen.

Ihr Nutzen

- **Bestmöglicher Schutz:** Sichere Abdeckung Ihrer Infrastruktur zu jeder Zeit
- **Minimiertes Risiko:** Individuelle Anpassung an die Sicherheitsbedürfnisse Ihres Unternehmens
- **Expertise und Entlastung:** Fachkundige Überwachung entlastet Ihr internes Personal
- **Compliance-Sicherheit:** Unterstützung bei der Einhaltung gesetzlicher Bestimmungen
- **Klare Kostenstruktur:** Transparente Preisgestaltung ohne unerwartete Zusatzkosten
- **Kontinuierliches Monitoring:** Die Sicherheitsüberwachung erfolgt permanent, idealerweise im 24/7-Betrieb.
- **Management von Sicherheitstools:** Effizientes Steuern und Warten von Sicherheitssystemen
- **Schnelle Alarmierung:** Schnelle Benachrichtigung bei detektierten Sicherheitsanomalien
- **Incident-Response (CSIRT):** Effiziente Eindämmung und Bewältigung von Sicherheitsvorfällen
- **Detailliertes Reporting:** Umfangreiche Berichterstattung über Sicherheitsereignisse und ergriffene Maßnahmen
- **Reporting:** Wir erstellen Berichte, die genau auf die Anforderungen Ihres Managements zugeschnitten sind.
- **Bedarfsorientierte Analyse und individuelle Konzeption:** Wir identifizieren Ihre spezifischen Sicherheitsbedürfnisse und passen unsere Konzepte entsprechend an.
- **Integration und Implementierung:** Nahtlose Integration in Ihre bestehenden Sicherheitsinfrastrukturen
- **Einhalten hoher Compliance-Anforderungen:** Wir orientieren uns strikt an den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI), um ein Maximum an Sicherheit zu gewährleisten.
- **Option eines zertifizierten Betriebs:** Die Durchführung erfolgt in deutschen Rechenzentren mit Zertifizierung oder auf Ihren eigenen Systemen.

Microsoft Defender

Bewahren Sie Ihr Unternehmen vor den Gefahren des digitalen Zeitalters – mit den Microsoft Defender-Lösungen. In einer Welt, in der Cyberkriminelle kontinuierlich neue Wege suchen, um in Unternehmensnetzwerke einzudringen und sensible Daten zu stehlen, ist es von entscheidender Bedeutung, robuste Abwehrmaßnahmen zu ergreifen.

Die Microsoft Defender-Lösungen bieten Ihnen genau das – eine zuverlässige und leistungsstarke Sicherheitslösung, die Ihre digitalen Assets schützt und Ihre geschäftlichen Aktivitäten vor den Folgen von Cyberangriffen bewahrt. Mit den verschiedenen Defender-Lösungen bietet Microsoft Ihnen Security-Lösungen, welche jeweils auf die verschiedenen Sicherheitsbedürfnisse von Unternehmen spezialisiert sind – ob Microsoft Defender for Endpoint zum Schutz Ihrer Endgeräte, Defender for Office für erweiterte Schutzmechanismen zur proaktiven Vermeidung von Phishing-Angriffen, Defender for Identity für die Sicherheit Ihrer digitalen Identität oder Defender for Cloud Apps für Ihre Cloud-Anwendungen: Microsofts Security-Lösungen sorgen für eine erhöhte Sicherheit Ihres Unternehmens.

Microsoft Defender for Endpoint

Schützen Sie Ihre Endpunkte mit einer der fortschrittlichsten Sicherheitslösungen auf dem Markt: Als Teil der integrierten Microsoft Endpoint Security Suite bietet der Microsoft Defender for Endpoint Unternehmen umfangreiche Schutzfunktionen, um die IT-Sicherheit zu verbessern und Bedrohungen effektiv zu bekämpfen. Das Beste daran? Der Microsoft Defender for Endpoint ist benutzerfreundlich, einfach zu installieren und konfigurieren. Mit flexiblen Bereitstellungsoptionen – einschließlich cloudbasiertem und lokal gehostetem Deployment. Der Defender for Endpoint unterstützt zudem eine Vielzahl von Plattformen und Betriebssystemen, einschließlich Windows, macOS, Linux und Android.

Ihr Nutzen

- **Rundumschutz:** Umfassender Schutz gegen eine Vielzahl von Bedrohungen, wie Malware, Ransomware, Spyware und andere Angriffe
- **Echtzeitbedrohungserkennung:** Reagieren Sie in Echtzeit auf Bedrohungen – nicht erst dann, wenn es bereits zu spät ist.
- **Automatisierte Reaktion auf Bedrohungen:** Bedrohungen schneller beseitigen und die Auswirkungen auf das Unternehmen minimieren
- **Zentrale Verwaltung:** Die Sicherheit Ihrer Endpunkte für Sicherheitsrichtlinien effektiver verwalten
- **Integration mit anderen Microsoft-Sicherheitsprodukten:** Umfassende Sicherheitslösung durch nahtlose Integration mit anderen Microsoft-Sicherheitsprodukten
- **Erweiterte Berichterstellung:** Bedrohungen und Sicherheitsrisiken mithilfe von erweiterten Berichterstellungsfunktionen identifizieren und bewerten

Microsoft Defender for Office

Der Microsoft Defender for Office ist eine fortschrittliche Sicherheitslösung, die speziell entwickelt wurde, um IT-Bedrohungen in Echtzeit zu erkennen und zu blockieren. Dank der intelligenten Technologie ist der Defender for Office eine der besten Sicherheitslösungen für Microsoft Office-Anwendungen und -Dienste auf dem Markt. Durch die nahtlose Integration in Office 365 und Microsoft 365 bietet er eine umfassende Abdeckung und schützt Ihr Unternehmen zuverlässig vor Bedrohungen. Die einfache Installation und Konfiguration machen den Defender for Office zur idealen Wahl für Unternehmen jeder Größe, die sich eine effektive und benutzerfreundliche Sicherheitslösung wünschen.

Ihr Nutzen

- Echtzeit-Erkennung verdächtiger Aktivitäten und ungewöhnlicher Verhaltensmuster sowie Blockierung von Bedrohungen
- Zugriff auf den Microsoft Intelligent Security Graph, um aktuelle Informationen über Bedrohungen und Angriffsmuster zu erhalten
- Sichere Überprüfung von E-Mail-Anhängen vor der Zustellung – dank des Safe Attachments Services
- Untersuchung von URLs in E-Mails auf schädliche (Phishing-)Inhalte mit dem Safe Links Service
- Nahtlose Integration in Office 365 und Microsoft 365 und umfassende Sicherheitsabdeckung für Microsoft-Office-Anwendungen

- Zentrale Verwaltung und Überwachung
- Benutzerfreundliche Installation und Konfiguration
- Flexible Bereitstellungsoptionen, einschließlich cloudbasierten und lokal gehosteten Deployment-Optionen
- Unterstützung für verschiedene Plattformen und Betriebssysteme, einschließlich Windows, macOS, iOS und Android
- Optimierte Kostenreduktion
- Kostenkontrolle

Microsoft Defender for Identity

Im digitalen Raum sind Identitäten das Tor zu Ihren Unternehmensressourcen – und damit auch zu internen Prozessen sowie sensiblen Daten. Schützen Sie Ihre Benutzeridentitäten sowie Ihre Unternehmensinfrastruktur vor den stetig wachsenden und sich verändernden digitalen Bedrohungen: Mit dem Microsoft Defender for Identity reduzieren Sie das Risiko von Cyberangriffen mit dem Ziel des Identitätsdiebstahls und nutzen gleichzeitig Ihre IT-Ressourcen effizienter. Die enge Integration in das Microsoft-Ökosystem und die Nutzung von fortschrittlichen Technologien machen diese Lösung zu einem effektiven Werkzeug.

Ihr Nutzen

- Überwachung von Benutzeraktivitäten
- Erkennen von verdächtigen und anomalen Aktivitäten
- Schutz vor Cyberangriffen
- Risikobewertung und Aufdecken von Sicherheitslücken
- Automatisierte Untersuchung von Sicherheitsvorfällen
- Automatisierte Reaktion auf Sicherheitsvorfälle
- Verbesserter Schutz Ihrer IT
- Effizientes Risikomanagement
- Optimierung der IT-Ressourcen
- Einfache Integration in die bestehende Microsoft-Infrastruktur
- Fortschrittliche Technologie auf Basis von Künstlicher Intelligenz und maschinellem Lernen

Microsoft Defender for Cloud Apps

In Zeiten von allgegenwärtigen Datenverstößen und Angriffen auf Unternehmensressourcen ist ein zuverlässiger IT-Schutz unerlässlich. Mit Microsoft Defender for Cloud Apps haben Sie die Gewissheit, dass Ihre Cloud-Anwendungen effektiv vor Malware, Angriffen und anderen Bedrohungen geschützt sind. Die Lösung bietet eine umfassende Sicherheitsstrategie, die sich nahtlos in Ihre bereits vorhandene Cloud-Infrastruktur integriert. Verlassen Sie sich auf den branchenführenden Schutz und konzentrieren Sie sich auf das Wachstum Ihres Unternehmens. Gerne beraten wir Sie bei der Implementierung und stellen sicher, dass Sie den optimalen Schutz für Ihre Cloud-Anwendungen erhalten.

Ihr Nutzen

- Umfassender Schutz Ihrer wertvollen Unternehmensressourcen
- Erweiterte, proaktive Bedrohungserkennung
- Intelligente Sicherheitsanalysen
- Identifizierung verdächtiger Aktivitäten, bevor sie zur Gefahr werden
- Kontinuierliche Überwachung des Datenverkehrs
- Volle Kontrolle über den Datenschutz inkl. Data Loss Prevention
- Einfache Integration in führende Cloud-Plattformen
- Benutzerfreundliche Verwaltungsoberfläche
- Festlegung von Richtlinien auf Basis von Standort, Gerät oder Benutzerrolle
- KI-gestützte Angriffserkennung selbst komplexester Angriffsmuster

Network

Im digitalen Zeitalter entsteht Innovation durch Kreativität. Wir stellen uns eine Welt vor, in der Technologie über das bloße Unterstützen unserer Tätigkeiten hinausgeht und stattdessen die Grundlage für mobile und digitale Technologien liefert, die die Art und Weise, wie wir uns vernetzen, revolutionieren.

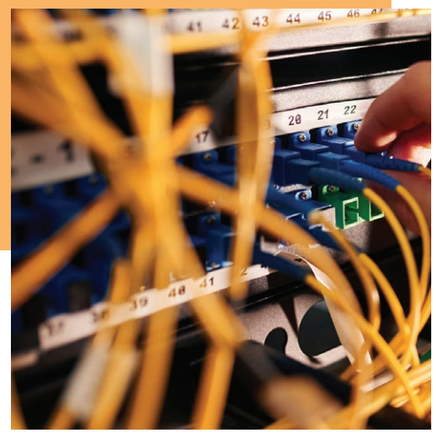
Die Netzwerkinfrastruktur stellt dabei das „zentrale Nervensystem“ von Unternehmen – und damit die essenzielle Grundlage für den Geschäftsbetrieb – dar. Denn erst dadurch wird eine effektive Kommunikation und Dienstleistung zwischen Usern, Diensten, Geräten etc. möglich. Allerdings nur dann, wenn hohe Verfügbarkeiten und Geschwindigkeiten gewährleistet werden können und das Netzwerk vor internen und externen Bedrohungen abgesichert ist.

Nutzen Sie die Ressourcen Ihres Netzwerkes bereits voll aus? Wir unterstützen Sie in allen Bereichen der Netzwerkinfrastruktur mit Know-how und Erfahrung.
Unsere Network-Leistungen für Sie:

- **Netzwerkanalyse:** Prüfung und Bewertung des IST-Zustandes Ihrer Netzwerkqualität, Identifizierung und Analyse von Schwachstellen sowie die Definition eines konkreten Maßnahmenplans zur Qualitätsverbesserung.
- **Netzwerk-Switch-Technologie:** Hohe Perfomance, 99,99%ige Verfügbarkeit, Sicherheit und Usability für Unternehmensnetzwerke und Rechenzentren. Die Vorteile erhalten Sie durch Zugriffs-, Rechenzentrums-, Core- und Aggregations-Switches.
- **Access Points und Controller:** In anspruchsvollen Unternehmensumgebungen zentralisieren WLAN-Controller das Management, die Richtlinien und die Access Points vor Ort, um die Leistung und Transparenz zu verbessern.
- **Netzwerkverwaltung:** Managementlösungen für die Netzwerkadministration liefern detaillierte Einblicke und vorausschauende Analysen für Unternehmen aller Größen – lokal und in der Cloud.
- **Netzwerksicherheit:** Unsere Lösungen schützen die Funktionsfähigkeit und Integrität Ihres Netzes sowie Ihrer Daten. Sie bieten mehr Transparenz, automatisierte Kontrollen und KI-gestützte Erkenntnisse für das integrierte Framework.

Seit vielen Jahren pflegen wir eine herausragende Partnerschaft mit einem der führenden Hersteller im Bereich Netzwerkinfrastruktur: HPE Aruba Networking. Durch die hervorragende Qualität sowie kontinuierliche Weiterentwicklung moderner und innovativer Produkte bietet HPE Aruba Networking die Grundlage, damit wir gemeinsam als kompetente und erfahrene Größen im Network-Fachgebiet stets die bestmögliche Lösung für Ihr Unternehmen und dessen Netzwerkbedürfnisse bereitstellen können.

LAN



Aruba Network Switches

Mit zunehmender Bedeutung der Digitalen Transformation für die moderne Geschäftswelt ist ein Faktor essenziell und damit entscheidend: die Konnektivität. Damit Computer, Drucker sowie andere Geräte – und somit Ihre Mitarbeitenden – genau das tun können, was sie tun sollen, ist eine robuste und leistungsfähige LAN-Infrastruktur unabdingbar. Hier kommt HPE Aruba Networking ins Spiel: Unser langjähriger Partner bietet erstklassige LAN-Produkte und -Technologien, die moderne Netzwerke effizienter und sicherer machen. Entscheiden Sie sich für HPE Aruba Networking – und setzen Sie damit auf eine Lösung, die Ihnen höchste Performance sowie eine einfache Verwaltung, umfassende Sicherheit und Energieeffizienz bietet. Mit fortschrittlichen Technologien, flexiblen und skalierbaren Lösungen und einer benutzerfreundlichen zentralen Managementplattform sind die Switches von HPE Aruba ideal für moderne Unternehmen, die eine robuste und zuverlässige Netzwerkinfrastruktur benötigen.

Switches

Hohe Bandbreite, geringe Latenz und schnelle Datenverarbeitung: Die Switches von HPE Aruba bieten eine herausragende Performance, die den Anforderungen moderner Netzwerke gerecht wird, und sorgen damit für eine zuverlässige und stabile Netzwerkverbindung. Egal, ob in kleinen Büros oder großen Rechenzentren (Campus oder Datacenter): HPE Aruba Switches gewährleisten eine nahtlose und unterbrechungsfreie Datenübertragung. Denn mit Unterstützung für Multi-Gigabit-Ethernet, PoE (Power over Ethernet) und SDN (Software-defined Networking) bieten sie die notwendige Flexibilität und Leistung – auch für anspruchsvolle Anwendungen und Umgebungen.

Profitieren Sie von hoher Flexibilität und Skalierbarkeit, die sich an die sich ständig ändernden Anforderungen Ihres Unternehmens anpassen lassen: Mit einer breiten Palette an Switches, die verschiedene Port-Dichten und Geschwindigkeiten bieten, können Netzwerke problemlos erweitert und an individuelle Bedürfnisse angepasst werden. Ein besonderes Highlight für wachsende Unternehmen und dynamische IT-Umgebungen: Die Switches sind sowohl Cloud- als auch On-Premises-fähig. Somit wird keine unterschiedliche Hardware benötigt; stattdessen kann jederzeit flexibel von einer

On-Premises- zu einer Cloud-Lösung und umgekehrt gewechselt werden. Sicherheit ist ein entscheidender Faktor in modernen Netzwerken: HPE Aruba integriert fortschrittliche Sicherheitsfunktionen in seine Switches, darunter rollenbasierte Zugriffskontrollen, eingebettete Firewalls und Bedrohungserkennung. Diese Maßnahmen schützen das Netzwerk vor unbefugtem Zugriff und Cyberbedrohungen, indem sie eine sichere Umgebung schaffen, die sensible Daten zuverlässig schützt. Die kontinuierliche Weiterentwicklung sowie regelmäßige Software-Updates von HPE Aruba gewährleisten zudem, dass Ihr Netzwerk stets auf dem neuesten Stand bleibt und zukünftige Anforderungen problemlos bewältigt werden können. Die Investition in Aruba Switches bedeutet, in eine langfristige und zukunftssichere Netzwerklösung zu investieren.

All das macht Aruba Switches attraktiv für den Einsatz in modernen Büros, Rechenzentren und Industrieanwendungen. Funktionen wie Energy Efficient Ethernet (EEE) und dynamische Energieverwaltung tragen zudem dazu bei, den Energieverbrauch der Switches zu optimieren; dies kann nicht nur zur nachhaltigen Reduzierung des ökologischen Fußabdrucks beitragen, sondern auch zur Senkung der Betriebskosten.

Aruba Central

HPE Aruba Networking setzt mit Aruba Central auf ein benutzerfreundliches Managementtool, welches eine zentrale Verwaltung der gesamten Netzwerkumgebung ermöglicht: Mit dem intuitiven Dashboard und den automatisierten Funktionen von Aruba Central können IT-Teams Netzwerke und Netzwerkgeräte effizient überwachen, konfigurieren und verwalten. Darüber hinaus kann die Betriebseffizienz gesteigert werden, indem wiederkehrende Aufgaben – wie z.B. die Validierung von Konfigurationen oder die schnelle Implementierung von Änderungen – automatisiert werden. Die Zusammenarbeit im IT-Team wird durch eine zentrale Ansicht und Versionskontrolle von Netzwerkkonfigurationen unterstützt.

Ihr Nutzen

- Höchste Performance und Zuverlässigkeit
- Einfache Verwaltung und Automatisierung
- Fortschrittliches Netzwerkmanagement mit Aruba Central
- Umfassende Sicherheitslösungen
- Regelmäßige Sicherheitsupdates
- Flexibilität und Skalierbarkeit
- Energieeffizienz und Nachhaltigkeit
- Integration fortschrittlicher Technologien
- Zukunftssichere Investition

Die zentrale Verwaltungsplattform Aruba Central ist in der Welt von HPE Aruba das Herzstück der Netzwerkverwaltung. Mehr zu der Lösung erfahren Sie auf S. 44.

SIEVERS Netzwerkkonzeptionierung

Sie möchten Ihr bestehendes LAN oder WLAN erneuern oder Sie planen, neue Netzwerkprodukte aus dem Hause HPE Aruba Networking zu implementieren? Sehr gut! Schließlich ist ein stabiles, leistungsfähiges und zukunftssicheres Netzwerk die Grundlage für einen intakten Geschäftsbetrieb. Doch wie können Sie eine solide und beständige Basis dafür schaffen? – Mit einem maßgeschneiderten Netzwerkkonzept, das die einzigartigen Anforderungen, Bedürfnisse und Herausforderungen Ihres Unternehmens berücksichtigt und Ihr Unternehmen somit maximal unterstützt: die SIEVERS Netzwerkkonzeptionierung.

Der Prozess der SIEVERS Netzwerkkonzeptionierung im Detail:

- **Erstgespräch und Bedarfsanalyse:** Der Startschuss fällt mit einem ausführlichen Gespräch, um Ihre aktuellen und künftigen Anforderungen zu verstehen. Dabei definieren wir gemeinsam mit Ihnen individuelle (Geschäfts-)Ziele.
- **Analyse der bestehenden Infrastruktur:** Wir überprüfen Ihre aktuelle Netzwerkinfrastruktur und identifizieren Verbesserungspotenziale.
- **Entwicklung des Netzwerkkonzepts:** Basierend auf den Analyseergebnissen entwickeln wir ein maßgeschneidertes Konzept für die Netzwerkarchitektur und -sicherheit und empfehlen Aruba-Produkte, die den Anforderungen nachkommen und die Netzwerkleistung maximieren.
- **Implementierungsplanung:** Neben dem Zeitplan koordinieren wir mit unserem Projektmanagement auch den Einsatz von Ressourcen sowie alle notwendigen Schritte, um einen reibungslosen Übergang zu gewährleisten.
- **Durchführung und Dokumentation:** Wir setzen das erarbeitete Netzwerkkonzept um und erstellen bei Bedarf eine umfassende Dokumentation.
- **Schulung und Support:** Um sicherzustellen, dass Sie mit der neuen Infrastruktur vertraut sind und diese effizient verwalten können, beziehen wir Ihre IT-Admins bei der Implementation mit ein. Darüber hinaus bieten wir Schulungen und fortlaufenden Support für Ihre (IT-) Mitarbeitenden.

Ihr Nutzen

- Optimierte und effiziente Netzwerkleistung
- Skalierbarkeit des Netzwerks
- IT-Sicherheit Ihrer Daten und Systeme vor Bedrohungen
- Minimierung von Ausfallzeiten und Wartungskosten
- Berücksichtigung individueller Geschäftsanforderungen
- Zukunftssicherheit
- Rundum-Service aus einer Hand

SIEVERS Netzwerksegmentierung

Optimieren Sie Ihre IT-Netzwerkstruktur durch intelligente Trennung – mit der SIEVERS Netzwerksegmentierung: Schließlich ist eine effiziente Netzwerksegmentierung in heutigen zunehmend komplexen Netzwerkumgebungen der Schlüssel zur Optimierung der Netzwerkleistung und -sicherheit.

Innerhalb des Segmentierungsprozesses wird ein großes Netzwerk in kleinere, überschaubare Segmente aufgeteilt – z.B. per physischer Segmentierung (Trennung durch physische Hardware, wie Router oder Switches) und logischer Segmentierung (Trennung innerhalb desselben physischen Netzwerks, z.B. durch VLANs, Subnetze oder andere logische Trennungen). Durch diese Segmentierung erzielen Sie eine gut strukturierte IT-Infrastruktur und können gezielt die Leistung, Sicherheit und Verwaltung Ihres Netzwerks verbessern. Darüber hinaus erhöhen Sie durch eine entsprechende Segmentierung auch die Sicherheit Ihres Netzwerks: Denn sollte ein Cyberangriff doch einmal erfolgreich sein, erlangen die Hacker nur Zugriff auf einzelne Segmente, in die sie eingefallen sind – nicht aber auf das vollständige Netzwerk.

Setzen Sie auf unsere Expertise und Erfahrung, um ein maßgeschneidertes Segmentierungskonzept zu erstellen, das Ihre spezifischen Anforderungen erfüllt und Ihr Netzwerk auf die Zukunft vorbereitet: Unsere Dienstleistungen im Rahmen der Netzwerksegmentierung helfen Ihnen, sicherzustellen, dass Ihr Netzwerk effizient und sicher betrieben wird.

Der Prozess der SIEVERS Netzwerksegmentierung im Detail:

- **Ermittlung der Anforderungen:** Ermittlung spezifischer Anforderungen für die Segmentierung; einschließlich der benötigten Sicherheitsstufen, Leistungsanforderungen und Benutzeranforderungen
- **Analyse der bestehenden Infrastruktur:** Prüfung der bestehenden Infrastruktur und Identifikation von Bereichen, die von einer Netzwerksegmentierung profitieren könnten
- **Segmentierungsstrategie:** Entwicklung einer maßgeschneiderten Segmentierungsstrategie, die Ihre Geschäftsziele und IT-Anforderungen berücksichtigt
- **Implementierung:** Umsetzung der Segmentierungsstrategie, einschließlich der physischen und logischen Trennung, Konfiguration von VLANs, Subnetzen und anderen Segmentierungstechniken sowie Zugriffsrichtlinien
- **Sicherheitsoptimierung:** Feinabstimmung der Sicherheitsrichtlinien und Implementierung von Überwachungs- und Managementtools
- **Dokumentation:** Erstellung einer umfassenden Dokumentation, die die Struktur und die Richtlinien der Segmentierung beschreibt
- **Schulung:** Durchführung von Schulungen für Ihre IT-Mitarbeitenden zur Verwaltung und Überwachung der neuen Netzwerkstruktur

Ihr Nutzen

- Isolation von Sicherheitsbedrohungen
- Bessere Kontrolle über Zugriff auf sensible Daten und Systeme
- Verbesserte Netzwerkleistung
- Effizientere Verwaltung des Netzwerkverkehrs
- Reduktion von Leistungsengpässen
- Vereinfachung der Netzwerkverwaltung
- Ermöglichung einer gezielten Überwachung und Fehlersuche
- Einfache Erweiterung und Anpassung des Netzwerks möglich

WLAN

Aruba Access Points

Eine zuverlässige und leistungsstarke WLAN-Verbindung ist heute unerlässlich – denn diese bildet in vielen Unternehmen die Grundvoraussetzung für verschiedene Geschäftsprozesse, die interne und externe Kommunikation sowie die allgemeine (Zusammen-)Arbeit. Egal, ob kleines Unternehmen, großer Konzern oder öffentliche Einrichtung: Mit den WLAN-Produkten von HPE Aruba Networking – einem der führenden Anbieter im Bereich Netzwerktechnologie – sind Sie bestens gerüstet, um den Herausforderungen der digitalen Gegenwart und Zukunft zu begegnen.

Die modernen WLAN-Lösungen von Aruba bieten eine herausragende Performance, blitzschnelle Datenübertragungen und eine stabile, unterbrechungsfreie Verbindung – selbst in Umgebungen mit hoher Gerätedichte –, und können damit sowohl die Produktivität Ihrer Mitarbeitenden als auch die Zufriedenheit Ihrer Kunden steigern.

Setzen Sie auf eine fortschrittliche Technologie mit einem innovativen Design und benutzerfreundlicher Oberfläche. Die WLAN-Produkte bieten eine hervorragende Benutzererfahrung: Mit Funktionen wie ClientMatch und AppRF können Access Points intelligent verwaltet und Anwendungen priorisiert werden, um eine reibungslose und qualitativ hochwertige Verbindung zu gewährleisten. Dies ist besonders wichtig in Umgebungen wie Konferenzzentren, Universitäten oder Krankenhäusern, wo eine Vielzahl von Geräten gleichzeitig auf das Netzwerk zugreift. Zudem wird dank der AirMatch-Technologie die Funkfrequenznutzung automatisch optimiert, um eine bestmögliche Leistung zu gewährleisten. Zusätzlich tragen Green AP-Funktionen dazu bei, den Energieverbrauch zu senken, indem sie Access Points in Zeiten geringer Nutzung in den Energiesparmodus versetzen.

Alle Access Points bieten die Möglichkeit der Triangulation: Durch die Messung der Entfernung des Clients zu den (mindestens) drei Access Points kann der Standort des Clients bis auf wenige Meter genau bestimmt werden. Diese Funktion ist besonders nützlich in großen Einrichtungen oder Campusumgebungen, um eine genaue Lokalisierung und Verwaltung von Geräten zu ermöglichen. Die Access Points der 6er-Serie verfügen zudem über eine integrierte GPS-Funktion. Diese ermöglicht eine präzise geografische Lokalisierung der Access Points selbst, was die Planung und Verwaltung des Netzwerks erheblich erleichtert.

Last, but not least können die WLAN-Produkte von HPE Aruba Networking auch den wachsenden Sicherheitsanforderungen moderner Netzwerkwelten gerecht werden: So werden u.a. fortschrittliche Sicherheitsfunktionen wie eingebettete Firewalls, Bedrohungserkennung und -abwehr sowie rollenbasierte Zugriffskontrollen standardmäßig in die Produkte integriert. Damit schützen Sie sensible Daten vor unbefugten Zugriffen.

Ihr Nutzen

- Hervorragende Performance & Zuverlässigkeit
- Einfache Verwaltung & Skalierbarkeit
- Sicherheit auf höchstem Niveau
- Optimierte Benutzererfahrung
- Effizienz & Nachhaltigkeit
- Präzise Standortbestimmung & GPS-Funktion
- Innovatives Design
- Fortschrittliche Technologie
- Zukunftssichere Investition
- Benutzerfreundliche Verwaltungsplattform

Weitere Vorteile für Ihr WLAN bietet außerdem die benutzerfreundliche Verwaltungsplattform Aruba Central: Die Cloud-basierte Lösung ermöglicht eine einfache und zentrale Verwaltung des gesamten Netzwerks. Mehr zum Netzwerkmanagement mit Aruba Central lesen Sie auf S. 44.

SIEVERS WLAN-Ausleuchtung

In einer immer stärker vernetzten Arbeitswelt ist eine professionelle und sorgfältige WLAN-Ausleuchtung der Schlüssel zu einem leistungsstarken und zuverlässigen WLAN-Netzwerk: Denn damit wird sichergestellt, dass sich alle Bereiche einer Einrichtung – egal, ob Büro, Lagerhalle, Krankenhaus oder Schule – auf eine optimale und gleichmäßige WLAN-Abdeckung verlassen können.

Unser professioneller Managed Service im Bereich WLAN-Ausleuchtung basiert auf modernsten Techniken und hilft Ihnen, diese bestmögliche Netzabdeckung in Ihrem Unternehmen zu erzielen. Durch detaillierte Analyse, präzise Planung, umfassende Dokumentation und unter Berücksichtigung individueller Faktoren helfen wir Ihnen, Interferenzen zu minimieren, tote Zonen zu vermeiden und eine gleichmäßige Signalstärke in allen Bereichen sicherzustellen. Unser Service beinhaltet dementsprechend unter anderem:

- **Vor-Ort-Site-Survey:** Bei der detaillierten WLAN-Ausleuchtung vor Ort messen wir die Signalstärke, identifizieren Interferenzen und analysieren die Netzwerkauslastung, um die beste Platzierung der Access Points zu bestimmen.
- **Interferenzanalyse:** Mittels Identifizierung potenzieller Interferenzquellen können diese minimiert werden. Dies verbessert die Netzwerkleistung und reduziert Verbindungsabbrüche.
- **Heatmaps und Dokumentation:** Wir erstellen visuelle Heatmaps, die die Signalstärke und Abdeckung in verschiedenen Bereichen darstellen. Diese Dokumentation erleichtert die Identifizierung von toten Zonen und Bereichen mit schwacher Signalstärke.
- **Spektrumanalyse:** Unsere Analyse umfasst auch eine detaillierte Untersuchung des Frequenzspektrums, um Nicht-WIFI-Interferenzen zu erkennen und zu vermeiden.

Investieren Sie in die professionelle SIEVERS WLAN-Ausleuchtung und profitieren Sie von einer verbesserten Netzwerkleistung sowie zufriedenen Usern.

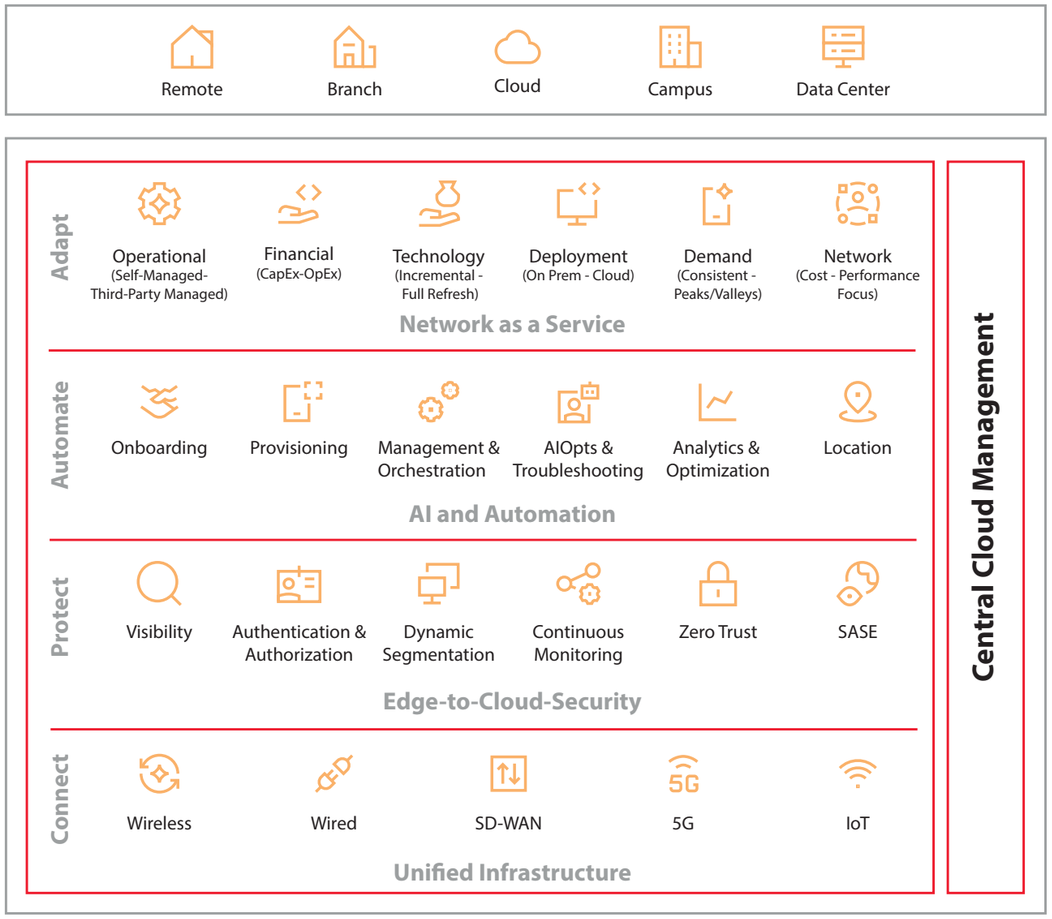
Ihr Nutzen

- Gleichmäßige Netzabdeckung in allen Bereichen Ihres Unternehmens
- Individuelle Planung auf Grundlage eines aktuellen Gebäudeplans
- Optimale und gleichmäßige Signalstärke für alle User
- Minimierung von Interferenzen durch andere elektronische Geräte oder benachbarte WLAN-Netzwerke
- Maximierung der Netzwerkleistung durch effiziente Kanalnutzung
- Flexible Anpassung der Lösungen an Größe und Anforderungen Ihres Netzwerks

Aruba Central (Netzwerk-management)

Eine effiziente Verwaltung und Überwachung der Netzwerkinfrastruktur ist in der digitalen Welt von heute unabdingbar – und die Wahl des richtigen Managementtools war noch nie so einfach: Die cloudbasierte Managementplattform Aruba Central aus dem Hause HPE Aruba Networking ist ein Allrounder in puncto Netzwerkmanagement – und Ihre Schaltzentrale für eine agile, sichere und effiziente Netzwerkinfrastruktur. Aruba Central bietet umfassende Lösungen für die Verwaltung, Überwachung und Sicherung von WLAN-, LAN- und SD-WAN-Netzwerken und wird damit den Anforderungen modernster Netzwerke gerecht.

Aruba Central ermöglicht eine zentrale Verwaltung aller Netzwerkkomponenten über eine intuitive, benutzerfreundliche Oberfläche. Egal, ob es sich um WLAN-Access Points, Switches oder SD-WAN-Geräte handelt: IT-Admins können das gesamte Netzwerk von einer einzigen Konsole aus überwachen, konfigurieren und verwalten – und das von überall aus. Dies vereinfacht nicht nur die Administration, sondern bietet auch einen umfassenden Überblick über die Netzwerkperformance und -gesundheit. Mit integrierten KI-gestützten Analysefunktionen bietet das Managementtool zudem tiefe Einblicke in die Netzwerkleistung und unterstützt Sie dabei, potenzielle Probleme proaktiv zu erkennen und zu beheben. Die Plattform nutzt maschinelles Lernen, um Muster zu erkennen und Anomalien zu identifizieren, was eine schnellere Fehlerbehebung und optimierte Netzwerkleistung ermöglicht. Zudem können wiederkehrende Aufgaben automatisiert werden, was den Verwaltungsaufwand erheblich reduziert. Auch Sicherheit ist ein zentrales Element: So stehen fortschrittliche Sicherheitsfunktionen wie rollenbasierte Zugriffskontrollen, integrierte Firewalls und Bedrohungserkennung zur Verfügung. Darüber hinaus ermöglicht Aruba Central die zentrale Verwaltung von Sicherheitsrichtlinien und die Implementierung von Zero-Trust-Sicherheitsmodellen, die den Schutz sensibler Daten gewährleisten. Die Managementplattform ist darauf ausgelegt, die Implementierung und Konfiguration von Netzwerkgeräten so einfach wie möglich zu gestalten. Mit Zero-Touch-Provisioning können neue Geräte automatisch konfiguriert und in Betrieb genommen werden, sobald sie mit dem



Netzwerk verbunden sind. Die Plattform bietet detaillierte Reporting- und Analysefunktionen, die es Unternehmen ermöglichen, die Netzwerkperformance und Benutzeraktivitäten genau zu überwachen. Mit benutzerdefinierten Dashboards und Berichten können IT-Administratoren die wichtigsten Leistungskennzahlen im Blick behalten und fundierte Entscheidungen zur Optimierung der Netzwerkinfrastruktur treffen. Aruba Central ist ein integraler Bestandteil der umfassenden Edge Services Platform (ESP) von HPE Aruba Networking. Diese Plattform bietet eine einheitliche Architektur für die Bereitstellung, Verwaltung und Sicherung von Netzwerken an der Netzwerkrandseite (Edge). Mit Aruba ESP können Unternehmen ihre Netzwerke effizienter gestalten, indem sie Künstliche Intelligenz und Automatisierung nutzen, um komplexe Aufgaben zu vereinfachen und die Netzwerkleistung zu optimieren. Aruba Central ermöglicht die nahtlose Integration und Verwaltung aller Komponenten innerhalb der ESP, was eine einheitliche und konsistente Netzwerkinfrastruktur gewährleistet. Last, but not last ist Aruba Central für Unternehmen jeder Größe geeignet – von kleinen Büros bis hin zu großen, verteilten Unternehmen. Die Plattform bietet die Flexibilität, mit den individuellen Anforderungen eines Unternehmens mitzuwachsen, ohne dass zusätzliche Hardware erforderlich ist. Neue Geräte können nahtlos integriert sowie bestehende Netzwerke problemlos erweitert werden.

Kurzum: Mit Aruba Central haben Sie die Kontrolle über Ihr Netzwerk in einer Hand – zentral, sicher und effizient.

Ihr Nutzen

- Verwaltung von Netzwerkelementen wie Access Points, Switches und Gateways von einem einzigen Dashboard aus
- Implementierung und Durchsetzung einheitlicher Richtlinien über Ihr gesamtes Netzwerk
- Schnelle Identifizierung und Behebung von Netzwerkproblemen – dank umfassender Überwachungs- und Diagnosefunktionen
- Automatisierung und Orchestrierung, um repetitive Aufgaben zu reduzieren und die Effizienz zu steigern
- KI-gestützte Analysen, um Netzwerkverhalten zu verstehen und vorausschauende Empfehlungen zu erhalten

Aruba ClearPass (Netzwerkzugangskontrolle)

Mit immer komplexeren Netzwerkarchitekturen und wachsenden Cyberbedrohungen nimmt die Arbeit in der IT-Abteilung Ihres Unternehmens zu – und wird herausfordernder. Doch mit geeigneten IT-Lösungen lässt sich der Mehraufwand Ihrer Mitarbeitenden reduzieren: z.B. mit der umfassenden Netzwerkzugriffskontrollsoftware Aruba ClearPass unseres Partners HPE Aruba Networking.

Aruba ClearPass ist eine leistungsstarke Plattform für die zentrale nahtlose Verwaltung, Überwachung, Sicherung und Optimierung Ihres Netzwerkzugriffs und bietet Ihnen damit die vollständige Kontrolle über alle Geräte (drahtlos wie kabelgebunden), User und Anwendungen innerhalb Ihres Netzwerks. Von der Identitätsverwaltung über die sichere Verwaltung von Gastzugängen bis hin zur Durchsetzung von Richtlinien bietet ClearPass eine robuste Sicherheitsinfrastruktur, die sich Ihren spezifischen Anforderungen anpasst. Die Integration des RADIUS-Protokolls und die Unterstützung für dynamische Segmentierung machen ClearPass zu einer besonders effektiven Lösung für die zentrale Verwaltung von Netzwerkzugriffen und die flexible Anpassung der Netzwerksicherheit.

Die Lösung ist skalierbar, herstellerunabhängig, lässt sich an die dynamischen Anforderungen moderner IT-Umgebungen anpassen und nahtlos in bestehende Netzwerkinfrastrukturen integrieren – und ist damit die richtige Wahl für Unternehmen jeder Größe und Branche.

Ihr Nutzen

- Umfassende Netzwerkzugriffskontrolle
- Rollenbasierte Zugriffssteuerung und -sicherung
- Dynamische Segmentierung
- Leistungsstarker RADIUS-Server
- Authentifizierung, Autorisierung und Abrechnung (AAA) für Netzwerkzugriffe
- Schutz des Netzwerkes vor unbefugtem Zugang und Fremdgeräten
- Herstellerunabhängige Lösung
- Geräte- und User-Erkennung
- Automatisierte Richtlinien- und Zugangsverwaltung
- Nahtlose Integration von Sicherheits- und Compliance-Richtlinien
- Sicheres, flexibles und benutzerfreundliches Gastmanagement
- Detaillierte Einblicke in die Netzwerkaktivität und -nutzung
- Nahtlose Integration in bestehende Netzwerk- und Sicherheitsinfrastrukturen (einschließlich WLAN, LAN und SD-WAN)
- Flexible und skalierbare Implementierung
- Umfassende Reporting- und Analysefunktionen
- Automatische VLAN-Zuordnung von Endgeräten
- Accounting/Profiling von Endgeräten
- Unterstützung für moderne Netzwerkarchitekturen

SIEVERS NAC-Workshop

Unser Workshop zur effizienten Netzwerkzugriffskontrolle mit Aruba ClearPass bietet Ihnen umfassende Einblicke und praxisorientiertes Expertenwissen, um die Vorteile dieser Lösung vollständig auszuschöpfen.

Die einzelnen Themen im Überblick

1. Einführung in Aruba ClearPass
- Überblick und Architektur
- Einsatzmöglichkeiten

2. Netzwerkzugangskontrolle mit ClearPass
- RADIUS-basierte Authentifizierung
- Dynamische Segmentierung

3. Policy Management
- Richtlinienerstellung
- Gastzugang

4. Integration und Automatisierung
- Integration in andere Sicherheitslösungen
- Automatisierte Workflows

5. Praktische Übungen
- Hands-on Lab
- Fehlerbehebung und Best Practices

Ihr Nutzen

- **Praxisorientiertes Lernen:** Erhalten Sie eine praxisnahe Schulung, die Ihnen hilft, das Gelernte direkt in Ihrer Umgebung anzuwenden.
- **Kompetenzentwicklung:** Erweitern Sie Ihre Kenntnisse im Bereich Netzwerkzugangskontrolle und Sicherheitsmanagement.
- **Netzwerken:** Tauschen Sie sich mit anderen IT-Profis aus und profitieren Sie von deren Erfahrungen und Best Practices.

SIEVERS Netzwerkanalyse / Troubleshooting

Langsame Verbindungen, Verbindungsabbrüche, unzureichende Bandbreite oder Sicherheitslücken: Wenn das Netzwerk auf Probleme oder Grenzen stößt, kann das die Produktivität Ihres Unternehmens beeinträchtigen – und Frustration bei den Nutzer:innen hervorrufen. Doch wie können Sie ein reibungslos funktionierendes und verfügbares Netzwerk sicherstellen? Individuelle Antworten darauf können wir Ihnen mit unseren Netzwerkanalyse- und Troubleshooting-Services liefern: Dabei bieten wir Ihnen umfassende Lösungen, um Netzwerkprobleme zu identifizieren, zu beheben, die Leistung Ihres Netzwerks zu optimieren – und die ideale Basis für einen reibungslosen Betrieb und produktive Arbeit zu schaffen.

Netzwerkanalyse: Unsere Netzwerkanalysen umfassen eine umfassende Überprüfung und Bewertung Ihrer gesamten Netzwerkinfrastruktur. Dabei identifizieren wir Schwachstellen, Engpässe und potenzielle Sicherheitsrisiken, um proaktive Maßnahmen zur Verbesserung der Netzwerkleistung und -sicherheit zu empfehlen.

Troubleshooting: Der Troubleshooting-Service zielt darauf ab, spezifische Probleme in Ihrem Netzwerk zu identifizieren und zu beheben. Es kommen modernste Tools und Techniken zum Einsatz, um die Ursache von Netzwerkproblemen schnell zu lokalisieren und zu beheben.

Proaktive Überwachung: Durch proaktive Netzwerküberwachung können wir potenzielle Probleme erkennen, bevor sie zu größeren Störungen führen. Unser Team überwacht Ihr Netzwerk und sorgt dafür, dass es stets optimal funktioniert. Bei Anomalien oder verdächtigen Aktivitäten werden sofort entsprechende Maßnahmen ergriffen.

Leistungsoptimierung: Wir analysieren die Leistung Ihres Netzwerks und identifizieren Bereiche, in denen Verbesserungen vorgenommen werden können. Durch die Optimierung von Netzwerkeinstellungen, die Aktualisierung von Hardware und Software sowie die Implementierung bewährter Verfahren stellen wir sicher, dass Ihr Netzwerk seine maximale Leistung erreicht.

Ihr Nutzen

- Schnelle Reaktionszeiten
- Effiziente Problemlösung und -behebung
- Minimierung von Ausfallzeiten
- Verbesserte, effiziente Netzwerkleistung
- Erhöhte Sicherheit

Aruba SD-WAN

Unternehmen sind zunehmend auf Cloud-Dienste und global verteilte Netzwerke angewiesen – damit wird eine leistungsstarke, flexible und sichere Netzwerkinfrastruktur unerlässlich.

Erleben Sie die Zukunft des Netzwerkmanagements mit einer Lösung, die auf intelligente und sichere Netzwerke ausgerichtet ist: Aruba SD-WAN ist die Antwort auf die Anforderungen moderner Netzwerke. Aruba SD-WAN bietet eine leistungsstarke, sichere und flexible Lösung für die Verwaltung und Optimierung moderner Netzwerke. Mit Funktionen zur Verbesserung der Cloud-Anwendungsleistung, intelligenten Netzwerkverwaltung, integrierten Sicherheit und zentralen Orchestrierung stellt Aruba SD-WAN sicher, dass Ihr Netzwerk den höchsten Leistungs- und Sicherheitsstandards entspricht. Durch die Möglichkeit, kostengünstige Internetverbindungen effektiv zu nutzen und die zentrale Verwaltung zu vereinfachen, bietet sich eine kosteneffiziente und zukunftssichere Lösung für die Netzwerkinfrastruktur Ihres Unternehmens. Mit der Unterstützung für dynamische Anpassungen und einer nahtlosen Integration in bestehende Systeme kann Ihr Unternehmen Netzwerkressourcen optimal nutzen und gleichzeitig die User-Erfahrung verbessern.

Ihr Nutzen

- Verbesserte Netzwerkzuverlässigkeit
- Optimierte Nutzung vorhandener Netzwerkressourcen
- Optimale Leistung für Cloud- und SaaS-Anwendungen
- Intelligente Netzwerkverwaltung und -überwachung
- Frühzeitiges Erkennen von Anomalien und Problemen
- Zero-Touch-Provisioning
- Flexible, skalierbare Architektur
- Durchgängige Sicherheitsstrategie für den Datenverkehr innerhalb des Netzwerks
- Abgesicherter Zugriff auf externe Cloud-Dienste
- Unterstützung von Zero-Trust-Sicherheitsmodellen
- Geringere Latenzzeiten
- Nahtlose Integration von Cloud-Anwendungen
- Zentrale Verwaltungsplattform für das gesamte WAN

Mehr Informationen zur zentralen Verwaltungsplattform Aruba Central erhalten Sie auf S. 44.

Aruba Security Service Edge (SSE)

In unserer zunehmend vernetzten Arbeitswelt sind Unternehmen auf eine Vielzahl von Cloud-Diensten und -Anwendungen angewiesen – damit gewinnt das Thema Sicherheit des Netzwerks immer mehr an Bedeutung. HPE Aruba Networking bietet mit seinem Security Service Edge (SSE) – ehemals bekannt als Axis – eine hochmoderne Sicherheitslösung, die speziell für die Anforderungen der modernen IT-Landschaft entwickelt wurde.

Durch die Kombination von SD-WAN und fortschrittlichen Sicherheitsfunktionen in einer Plattform ermöglicht Aruba SSE einen ganzheitlichen Schutz aller Netzwerkressourcen, optimiert die Netzwerkleistung und vereinfacht die Sicherheitsverwaltung.

Die Flexibilität, Skalierbarkeit und zentrale Verwaltung von Aruba SSE sorgen dafür, dass Ihre Netzwerksicherheit auf dem neuesten Stand bleibt und sich an die individuellen und sich ändernden Anforderungen Ihres Unternehmens anpasst. Durch die Zero-Trust-Network-Access-Funktionen kann Ihr VPN durch eine sichere Lösung ersetzt werden.

Ihr Nutzen

- Ganzheitlicher Schutz durch Security Service Edge
- Optimierung der Netzwerksicherheit
- Sicherer Web-Gateway (SWG)
- Zero Trust Network Access (ZTNA)
- Cloud Access Security Broker (CASB)
- Digital Experience Monitoring (DEM)
- Zentrale Verwaltung und Orchestrierung
- Zukunftssichere Sicherheitslösungen
- Leistungsstarke Sicherheits- und Netzwerkmanagement-Funktionen
- KI-gestützte Analysen
- Nahtlose Integration von SD-WAN und Sicherheitsfunktionen
- Effiziente und sichere Verwaltung des Netzwerks
- Intelligente Verkehrssteuerung
- Flexibilität und Skalierbarkeit für moderne Netzwerke
- Problemlose Integration in bestehende Netzwerkinfrastrukturen

Die SIEVERS-GROUP als Partner

Wir machen IT einfach – seit 1989.

Mehr als 350 Mitarbeitende machen die SIEVERS-GROUP an den Standorten Osnabrück und Kaarst bundesweit zu dem IT-Dienstleister, der er schon seit mehr als drei Jahrzehnten ist: Ihr kompetenter Partner für ganzheitliche IT-Architekturen. Darüber hinaus setzt die SIEVERS-GROUP seit jeher auf strategische Partnerschaften mit ebenso innovativen wie renommierten Herstellern, Technologieführern und Branchenspezialisten im In- und Ausland. Wenn Ihre IT läuft, haben Sie Freiheit und Ruhe, um sich konsequent auf Ihr Kerngeschäft fokussieren zu können.

Sie haben Interesse an unseren Produkten und Services und wünschen eine persönliche Beratung? Nehmen Sie Kontakt mit uns auf – wir freuen uns auf den offenen Austausch mit Ihnen.

SIEVERS-SNC Computer & Software GmbH & Co. KG
Ein Unternehmen der SIEVERS-GROUP
Hans-Wunderlich-Straße 8
49078 Osnabrück

Telefon: 0541 9493 0
info@sievers-group.com
www.sievers-group.com

Bei uns sind Sie auf der sicheren Seite:

Qualitäts-management-system

Informations-sicherheits-managementsystem

Datenschutz-Grundverordnung (DSGVO)

Cloud-Standard für Datenschutz

Business Continuity Management System (BCMS)

Projekt-management

Projekt-management

SIEVERS-SNC Computer & Software GmbH & Co. KG
Ein Unternehmen der SIEVERS-GROUP
Hans-Wunderlich-Straße 8 · 49078 Osnabrück

Telefon: 05 41 94 93 0
info@sievers-group.com
www.sievers-group.com

SIEVERS

all digital.