DOKOM21 Unified Thread Management

Das zentrale und intelligente Gefahren-management für Ihre Cyber-Security

DOKOM21 ist Ihr kompetenter Partner für Ihre Cyber-Security durch ein intelligentes und von DOKOM21 verwaltetes Unified Threat Management-System. Sie betreiben Ihr Netzwerk selbst? In dem Fall sollten Sie sich vor Cyber-Kriminalität und -Angriffen absichern. Doch welcher Schutz ist angemessen und sinnvoll? Dies hängt von vielen unterschiedlichen Faktoren wie Firmengröße, Anzahl der Mitarbeiter und der Bedrohungslage in Ihrer Branche ab.

Ihre Vorteile im Überblick

- ✓ zentrale, vereinheitlichte und intelligente Lösung für maximale Sicherheit
- ✓ Bereitstellung und Management der Lösung durch DOKOM21
- ✓ individuelle und flexible Zusammenstellung der benötigten Cyber-Security-Dienste
- ✓ realisiert auf Basis der deutschen Rechtssicherheit mit Hardware bei Ihnen vor Ort oder in unserem TÜV-zertifizierten Reliable-Data-Center

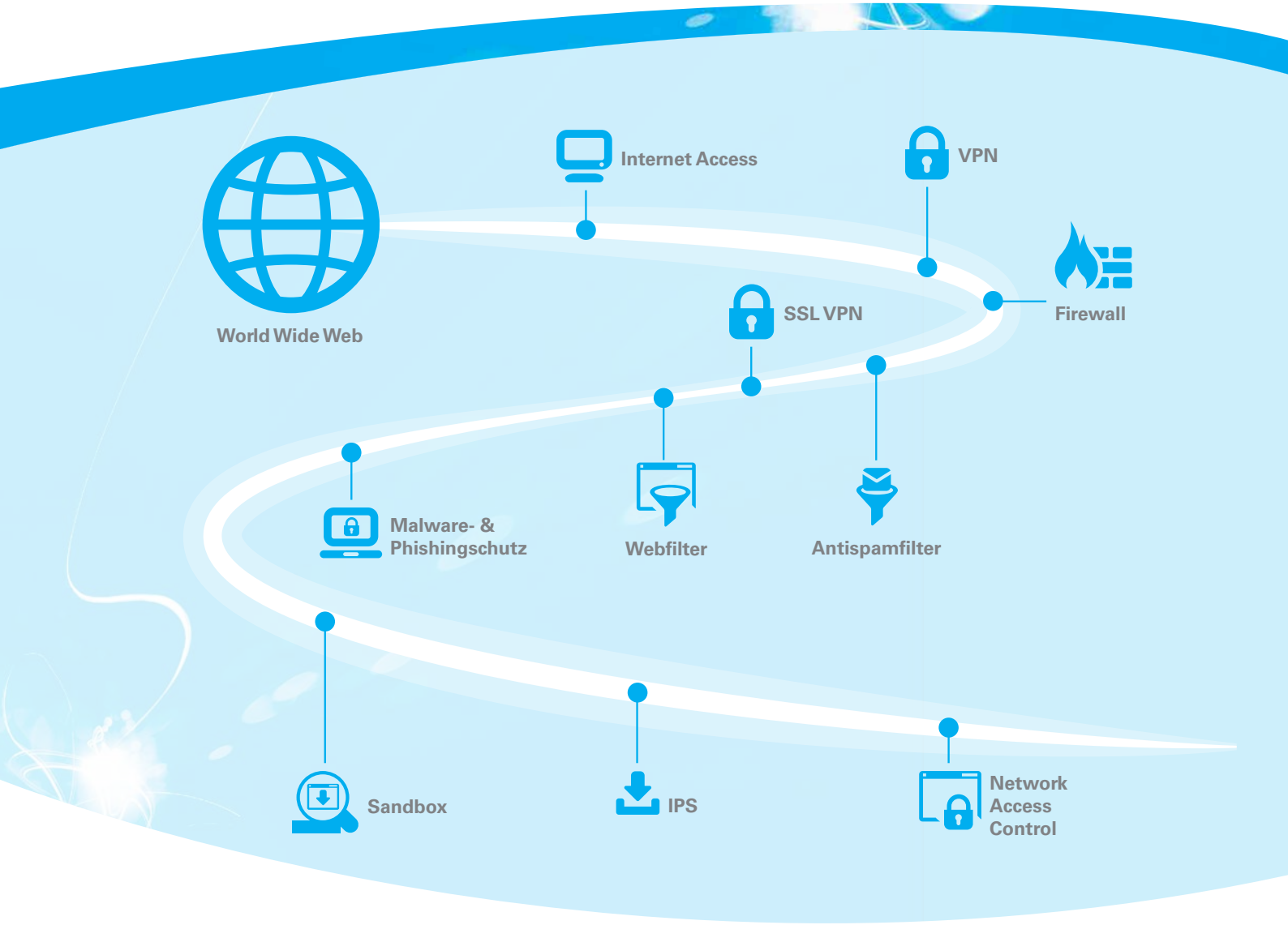
Warum DOKOM21?

- ✓ bester Service vor Ort: flexible und schnelle Reaktionszeiten
- ✓ 24 Stunden Störungsannahme und -bearbeitung
- ✓ breite Netzinfrastruktur über das Anschlussgebiet hinaus
- ✓ Ihre Businesslösung liegt kurzfristig auf Ihrem Schreibtisch
- ✓ jahrelange Erfahrung als Netzbetreiber und Dienstleister im Bereich Cyber-Security

Für welche Unternehmensgröße ist welcher Funktionsumfang ratsam?

Funktionsumfang	Dienste und Funktionen	Kleinunternehmen	Mittelständler	Konzern
1. Next Generation Firewall – Basisfunktion	✓ Netzwerkschutz ✓ Stateful Packet Inspection (SPI) ✓ Anti-Spoofing	zwingend notwendig	zwingend notwendig	zwingend notwendig
1.2 Next Generation Firewall – Erweiterte Funktion	✓ VPN-Gateway ✓ SSL VPN ✓ Application Control ✓ Demilitarisierte Zone (DMZ) ✓ Malware-Schutz ✓ Intrusion-Prevention Service (IPS)	notwendig	zwingend notwendig	zwingend notwendig
2. Secure E-Mail Gateway	✓ Malware-Schutz ✓ Anti-Spam ✓ Spoofing-Schutz ✓ Phishing-Schutz ✓ Schutz vor DoS-Angriffen ✓ User-Quarantäne	zu prüfen	notwendig	zwingend notwendig
3. Advanced Thread Protection	✓ Sandbox-Lösung ✓ Schutz vor Zero-Day Attacken	zu prüfen	zu prüfen	zwingend notwendig
4. Network Access Control	✓ Schutz der IT-Infrastruktur vor unbefugten Fremdgeräten	zu prüfen	zu prüfen	zwingend notwendig
5. Application Delivery Control	✓ Optimierung der Verfügbarkeit der Serverinfrastruktur	zu prüfen	zu prüfen	zu prüfen

0231. 930-94 02
www.dokom21.de



Ihr Schutz vor Cyber-Angriffen

- ✓ **Internet Access:**
  Internetzugang mit flexibel skalierbaren Geschwindigkeiten und optimal abgestimmten Tarifen, abhörsicher über Glasfaser
- ✓ **VPN:**
  Standortunabhängiger, dauerhaft eingerichteter, abgesicherter Zugang zum Unternehmensnetzwerk
- ✓ **SSL VPN:**
  Standortunabhängiger, temporär abgesicherter Zugang zum Unternehmensnetzwerk per Anmeldung über eine Clientsoftware
- ✓ **Next Generation Firewall:**
  Schutz des Unternehmensnetzwerkes vor unerwünschten internen und externen Zugriffen und Gefahren
- ✓ **Antispamfilter:**
  Schutz vor unerwünschten E-Mails zur Sicherung der Mail-Infrastruktur
- ✓ **Webfilter:**
  Individuelles Reglementieren bedenklicher und unerwünschter Webseiten, Dateitypen und Anwendungen
- ✓ **Malware- und Phishingschutz:**
  Schutz von Hardware und Systemen vor unbemerktem Eindringen durch Malware, Trojanern, Spyware, etc.
- ✓ **Sandbox:**
  Inhaltliche Prüfung des eingehenden Datenverkehrs in einer virtuellen Betriebsumgebung, um Veränderungen am Betriebssystem festzustellen
- ✓ **Intrusion Prevention Service:**
  System zur Erkennung von Angriffen als zusätzliche Kontrolleinheit zur Ergänzung der Firewall
- ✓ **Network Access Control:**
  Automatische Trennung des Ports bei Identifizierung von Gefahren durch Endgeräte, die das Netzwerk gefährden könnten

DOKOM Gesellschaft für Telekommunikation mbH
Stockholmer Allee 24 I 44269 Dortmund
Fon: 0231. 930-94 02 I Fax: 0231. 930-92 77
www.dokom21.de I E-Mail: info@dokom21.de

Was liegt näher... DOKOM21