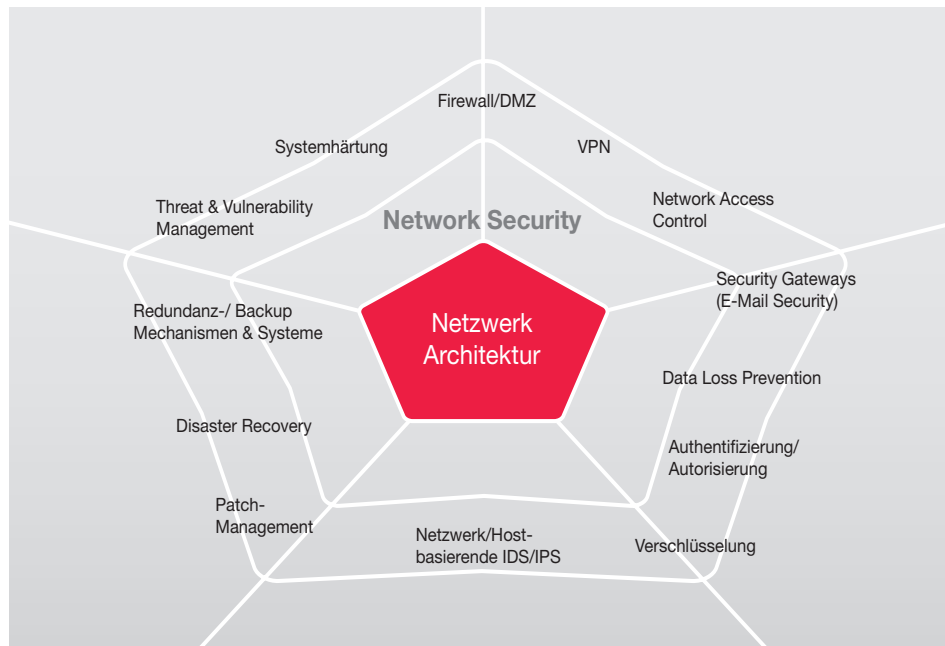


### Das Herzstück eines Unternehmens verlangt ganzheitlichen Schutz



#### Ihre Vorteile:

- » **Wirtschaftlich**
- » **Flexibel**
- » **Konsequent**
- » **Ganzheitlich**
- » **Aktuell**

Die heutige Unternehmenslandschaft ist extrem unterschiedlich, ihre IT-Landschaften sind es auch. IT-Netzwerke sind nicht nur in punkto Größe und Design, sondern auch im Hinblick auf geschäftskritische Prozesse unterschiedlich zu bewerten. **Das richtige Maß an Sicherheit sowie die geeigneten Sicherheitstechnologien zu finden, erfordert ein herstellerübergreifendes sowie langjähriges Fachwissen in beiden Bereichen: Sicherheit und Netzwerktechnologie.**

Vor dem Hintergrund des festgestellten Schutzbedarfs, beispielsweise durch unsere Analysen und Audits, überprüft secunet die bestehenden Sicherheitsmechanismen in Ihrem Unternehmen. Hierbei ist das Ziel, Ihre existierenden Strukturen soweit wie möglich zu optimieren und durch erforderliche Sicherheitsmechanismen in einem geeigneten Umfang zu ergänzen.

#### **Data Loss Prevention**

Durch eine Data Loss Prevention-Lösung werden Ihre Daten in vier Schritten automatisch gesichert und gegen Verlust durch internen Informationsabfluss geschützt.

- **Erkennen** – Sämtliche vertraulichen Daten werden gefunden und erfasst – unabhängig davon, wo sie gespeichert sind. Anschließend erfolgt eine automatische Verwaltung inklusive Datenbereinigung.
- **Überwachen** – Um einen unternehmensweiten Überblick zu erhalten, wird zusammengetragen, wie vertrauliche Daten verwendet werden, zum Beispiel ob Benutzer mit dem Unternehmensnetzwerk verbunden oder offline sind.
- **Schützen** – Es muss sichergestellt werden, dass vertrauliche Unternehmensdaten nicht nach außen gelangen können. Eine Übersicht über Richtlinienverstöße schützt die Daten präventiv.
- **Verwalten** – Die Definition universeller Richtlinien im gesamten Unternehmen hilft dabei, Richtlinienverstöße zu beheben und entsprechende Berichte und Inhalte zu erkennen.

Dabei ist es wichtig, das passende System für Ihre spezifischen Anforderungen zu finden. secunet hat langjährige Erfahrung in der Analyse sicherer Geschäftsprozesse und der Klassifizierung von Daten. Gepaart mit unseren umfangreichen Kenntnissen der im Markt erhältlichen DLP-Lösungen können wir Sie optimal bei der Auswahl und Integration unterstützen.

#### Firewall-Architektur

Bei jeder Netzwerköffnung, sei es zum Internet oder zu Partnernetzen, rücken Sicherheitsanforderungen in den Vordergrund. Firewall-Architekturen bieten hier einen wirksamen Schutz vor unberechtigtem Zugriff auf das Unternehmensnetz und seine sensiblen Daten. Zusätzlich ermöglichen sie eine Kontrolle der Verbindungen und über das Logging eine Auswertung der Internetnutzung bis hin zur Kostenzuweisung. Damit umfassen sie verschiedene Sicherheitszonen, die sich bezüglich Berechtigungen, Bedrohungen und Kontrollierbarkeit durch das Unternehmen in hohem Maße unterscheiden können. Um die Zugriffe zwischen diesen Sicherheitszonen zuverlässig zu reglementieren, werden Firewall-Systeme eingesetzt. secunet kennt die aktuellen Bedrohungen und Schwachstellen von IT-Systemen und berücksichtigt diese bei der Auswahl Ihrer passenden Firewall-Architektur.

#### Intrusion Detection and Intrusion Prevention Systeme

Die extreme Zunahme von System-Angriffen hat gezeigt, dass trotz des Schutzes durch Firewalls und Virens Scanner Netzwerke und Server empfindliche Schwachstellen aufweisen können. Vielen Unternehmen fehlt ein Instrument zur kontinuierlichen Erkennung, Überprüfung, Rückverfolgung und Vermeidung von Angriffen. Intrusion Detection oder Prevention Systeme (IDS und IPS) agieren in diesem Zusammenhang komplementär zu Ihren Firewalls, VPN-Gateways und Security Scannern. Grundlage für die Erkennung von Angriffen sind Audit- und Logfunktionen sowie Netzmonitore. Diese dokumentieren, wer wann und wo IT-sicherheitsrelevante Aktionen initiiert hat. Während ein IDS „passiv“ ausgelegt ist, d. h. einen Alarm auslöst oder einen Angriff protokolliert, greift ein IPS aktiv ein. Angriffe werden automatisch und unverzüglich blockiert, bevor ein Schaden überhaupt erst entstehen kann. Damit aber ausschließlich gefährliche Aktivitäten blockiert werden und der legitime Datenverkehr unbehindert bleibt, sind an die Genauigkeit der Systeme sowie einer bedarfsgerechten Einstellung hohe Anforderungen gestellt.

#### Virtuelle Private Netzwerke

Ein Virtuelles Privates Netzwerk (VPN) schützt die übertragenen Informationen vor unerwünschten Zugriffen, indem es einen „Tunnel“ durch unsichere Netzwerke (Internet, WAN, interne Netzwerke, etc.) aufbaut, der durch starke kryptographische Mechanismen abgesichert ist. VPNs können sowohl zur Standortvernetzung (Gateway-to-Gateway) als auch zum sicheren Zugriff eines mobilen Benutzers auf das Unternehmensnetzwerk über das Internet (Client-to-Gateway) eingesetzt werden. secunet implementiert geeignete VPN-Komponenten, die Ihre Anwendungen in vollem Umfang unterstützen und den Bedrohungen effizient entgegenwirken. Wir konfigurieren VPNs für Ihre individuellen Anforderungen, implementieren die Lösungen und unterstützen Sie beim dauerhaften Betrieb.

#### Warum secunet?

secunet ist führender Anbieter von IT-Sicherheitslösungen. Wir identifizieren individuell für jeden unserer Kunden die exakten Bedürfnisse und bieten ihnen maßgeschneiderte Sicherheit. Auf dieser Basis entwickeln wir ein spezielles Sicherheitskonzept, das für Ihr Unternehmensnetzwerk adäquat, skalierbar und effektiv ist. Wir übernehmen die Implementierung und gewährleisten einen dauerhaften Betrieb. Bei der Auswahl geeigneter Komponenten greifen wir auf eine große Anzahl an Produkten unserer Partner zurück, die wir bei Bedarf an Ihre spezifischen Anforderungen anpassen. Auch die Entwicklung neuer Komponenten ist kein Problem für unsere erfahrenen Spezialisten.

#### Ganzheitlicher Schutz Ihrer IT-Landschaft:

- **Wirtschaftlichkeit:**  
Optimierung und Ergänzung bestehender Sicherheitskomponenten
- **Konsequente Umsetzung:**  
Adressierung aller sicherheitsrelevanten Aspekte
- **Integration:**  
Ineinandergreifen der einzelnen Sicherheitskomponenten
- **Zentrales Management:**  
Reduzierung der Komplexität und des Administrationsaufwands
- **Flexibilität und Skalierbarkeit:**  
Im Rahmen des definierten Sicherheitsniveaus

Weitere Informationen:  
[www.secunet.com/nws](http://www.secunet.com/nws)

Factsheet Data Loss Prevention