

# *GRÜNES LICHT FÜR IHRE SICHERHEIT*



**NETZWERKSICHERHEIT**



## *Wir schützen Sie vor den Risiken öffentlicher Datennetze*



IT-Systeme sind die zentralen Ressourcen Ihres Unternehmens. Sie bilden die Basis Ihrer Geschäftsprozesse und Ihrer Wettbewerbsfähigkeit. Sichere, leistungsfähige und verfügbare IT-Infrastruktur ist gleichzeitig die Voraussetzung für Ihren erfolgreichen Eintritt in den E-Business-Markt.

Die Anbindung Ihres Unternehmensnetzes an öffentliche Netze birgt neben Chancen jedoch auch immer Risiken. Daher sind Security-Lösungen für sichere zuverlässige Verbindungen Ihrer privaten mit den öffentlichen Netzen unverzichtbar.

Angriffe auf Netzwerke und Systeme werden immer vielfältiger und gefährlicher. Sie reichen von der unbefugten Nutzung von Systemressourcen und den Angriffen durch Hacker bis zu Diebstahl und Manipulation von wichtigen Informationen und Daten.

IT-Security kann nicht mehr "nebenbei" abgewickelt werden. NESEC hat sich deshalb auf IT-Security spezialisiert und ein Team hochqualifizierter Experten zusammengestellt. Gemeinsam mit Ihnen definieren unsere Experten das erforderliche Sicherheitsniveau und beschreiben alle Maßnahmen, die eine lückenlose Sicherheit der Netzwerke und Systeme Ihres Unternehmens gewährleisten.

Unsere Spezialisten verfügen über langjährige Erfahrung in der Implementierung moderner Security-Lösungen, die aktuelle Risiken von Ihren Systemen und Netzwerken abwehren.

### **INSTALLATION UND KONFIGURATION**

Wir unterstützen Sie bei der Installation von Firewallsystemen. Wir liefern die Produkte, übernehmen die Installation und die Konfiguration sowie die Integration in Ihre Systemumgebung - alles aus einer Hand. Angefangen mit der sicheren Installation Ihrer Betriebssysteme über Ihre Firewall bis hin zur Ihrer Remote Access Lösung und dem unternehmensweiten VPN. Mit Hilfe von automatischen Angriffstools wird die installierte Lösung im Anschluß auf Sicherheitsschwächen überprüft.



## Erwehren Sie sich der Angriffe aus dem Internet

### FIREWALL



Mit jeder Netzwerköffnung, ob zum Internet oder zu Partnernetzen, rücken die Sicherheitsanforderungen in den Vordergrund. Firewalls bieten hier einen wirksamen Schutz vor unberechtigtem Zugriff auf Ihr Unternehmensnetz und Ihre schützenswerten, privaten Daten. Zusätzlich ermöglichen sie eine Kontrolle der Verbindungen und über das Logging eine Auswertung der Internetnutzung bis hin zur Kostenzuweisung.

Eine Firewall dient als "Schwelle" zwischen zwei Netzen, die überwunden werden muss, um Systeme im jeweils anderen Netz zu erreichen. Es wird dafür gesorgt, dass jede Kommunikation zwischen den beiden Netzen über die Firewall geführt werden muss. Auf der Firewall sorgen Zugriffskontrolle und Audit dafür, dass das Prinzip der geringsten Berechtigung durchgesetzt wird und potentielle Angriffe schnellstmöglich erkannt werden.

### VIRENSCHUTZ



Computerviren sind Programme, die sich selbst kopieren und per E-Mail, Datei- und Datenträgeraustausch oder direkt über Netzwerkverbindungen verbreiten. Viren richten Schäden an, indem sie Daten löschen oder verfälschen, Fehlkonfigurationen, Systemüberlastungen oder -abstürze herbeiführen. Die Sicherheit vor Virenbefall eines Computersystems hängt entscheidend von einer ganzheitlichen Sicherheitspolitik und einer konsequenten Systemadministration ab.

Virens Scanner sind Programme, die gezielt nach Viren suchen. Sie überwachen die Dateiablage auf zentralen Servern oder Arbeitsplätzen, prüfen regelmäßig alle abgelegten Programme und Dokumente auf Virenbefall und reparieren oder löschen betroffene Dateien. Allerdings ist ein Virens Scanner nur so gut wie er auch aktuell ist. NESEC überwacht auf Wunsch deshalb Ihr Netz durch ein maßgeschneidertes Sicherheitskonzept auf Viren- und Sicherheitsprobleme, führt Updates durch und behebt Sicherheitslücken.



## *Nutzen Sie die Möglichkeiten, die Ihnen das Internet bietet*

### **VIRTUAL PRIVATE NETWORKS**

Ein schneller Informationsaustausch zwischen Unternehmen, Außenstellen, mobilen Mitarbeitern und Geschäftspartnern ist heute unerlässlich für den Geschäftserfolg. Selbstverständlich muß auch dieser Informationsaustausch geschützt ablaufen. Um schnelle und preisgünstige Kommunikation über das Internet mit der Sicherheit von privaten Standleitungen zu kombinieren, wurde die Technologie des VPN (Virtual Private Network) entwickelt. Teure private Standleitungen können so durch die VPN-Technologie abgelöst werden. Die Investition in neue VPN-Produkte amortisiert sich in den meisten Fällen in kurzer Zeit.



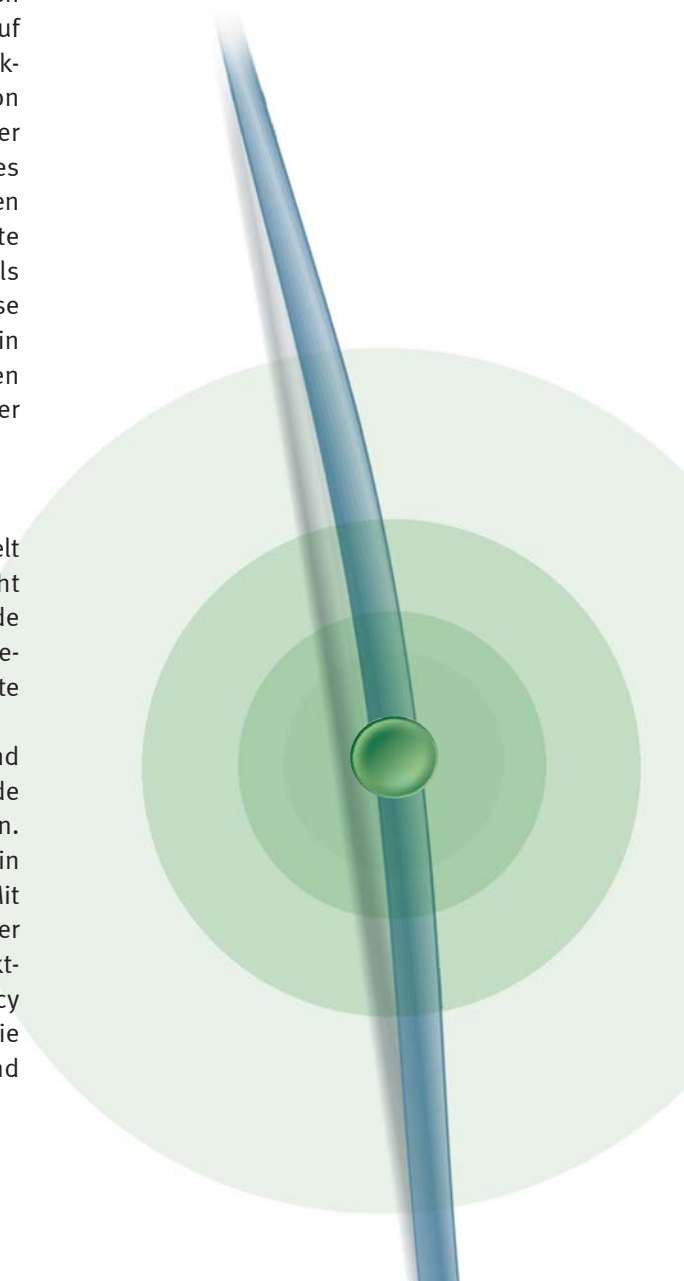
### **INTRUSION DETECTION**

Intrusion Detection Systeme (IDS) dienen dazu, Angriffe auf das Firmennetzwerk so früh wie möglich zu erkennen. Zwei verschiedene Arten von Intrusion Detection Systemen sind z. Zt. auf dem Markt verfügbar: host-basierte und netzwerk-basierte Systeme. Host-basierte Intrusion Detection Systeme werden auf dem Server installiert. Sie kontrollieren die Server-Logfiles und die auf dem Server laufenden Applikationen auf unautorisierte Zugriffe. Netzwerk-basierte Intrusion Detection Systeme fungieren als Agenten im Netzwerk in Form eines Sensors. Diese IDS filtern und analysieren Netzwerkpakete in Echtzeit und vergleichen sie mit bekannten Mustern von Attacken, die in einer dahinter liegenden Datenbank gespeichert sind.

### **SICHERHEITS- KONZEPTE**

Standardlösungen sind in der dynamischen Welt der Informationstechnologie von heute nicht gefragt. Jedes Security-Projekt ist anders, jede Installation stellt andere Anforderungen und benötigt andere, perfekt aufeinander abgestimmte Komponenten.

Unsere Konzeptionen sind sofort einsetzbar und lassen sich auch an das sich ständig verändernde technische und geschäftliche Umfeld anpassen. Eine Sicherheitslösung können wir jedoch nur in enger Zusammenarbeit mit Ihnen entwickeln. Mit unserem fundierten Know-how auf dem Gebiet der IT-Sicherheit übernehmen wir gerne die Projektleitung und Hauptarbeit. Die Security Policy gestalten wir in gemeinsamer Arbeit mit Ihnen. Die Beschlüsse werden von Ihnen getroffen und gemeinsam getragen.





## *Vertrauen Sie einem starken Partner*

Standardlösungen sind nur selten geeignet - erst Anpassungen machen verfügbare Lösungen einsatzfähig. Doch zunächst muß ein Unternehmen herausfinden, wo sich seine Sicherheitslücken befinden, wie es seine Informationen schützen kann und was die optimale Lösung ist. Dies erfordert einen IT-Sicherheitsberater, einen Marktkenner, einen Programmierer, einen IT-Fachmann zur Einführung der Lösung und einen Systemadministrator, der die tägliche Sicherheit im Unternehmen verantwortet - oder NESEC.

### **BERATUNG UND ANALYSE**

Immer komplexere Netzstrukturen und die Notwendigkeit, Anwendungen dezentral und über lokale Netzgrenzen hinaus zu betreiben, machen eine sorgfältige Bestandsaufnahme und Analyse der konkreten Anforderungen mit sachgerechter Konzeption zur Basis eines jeden IT-Security-Projektes.

Mit stets aktuellem technischen Wissen und praktischer Anwendungserfahrung stellen wir sicher, dass Ihre Netz- und Anwendungsstruktur den Sicherheitsanforderungen und den Bedürfnissen Ihrer betrieblichen Abläufe gerecht wird. Wir unterstützen Sie bei der Auswahl und Anpassung, aber auch beim Management von Sicherheitskomponenten in heterogenen Umgebungen.

### **MANAGED SECURITY**

Die meisten Unternehmer kennen die Gefahren des digitalen Geschäftslebens - Hacker, Viren oder sogar die eigenen Mitarbeiter. Je mehr Sie Ihr Unternehmen nach außen öffnen, desto anfälliger wird es für Angriffe. Trotzdem ist es vielerorts normal, geschäftskritische Daten beispielsweise unverschlüsselt per E-Mail zu verschicken.

Der Betrieb einer Sicherheits-Infrastruktur geht weit über das hinaus, was im klassischen Netzwerk-Infrastrukturbereich unter Betrieb zusammengefasst wird. Ausgebildete Spezialisten überprüfen ständig Protokolldateien. Potentielle Angriffe müssen sofort untersucht, nachverfolgt und bei Bedarf eliminiert werden. Neuveröffentlichungen von Sicherheitslücken müssen auf ihre Relevanz für die eigenen Dienste überprüft und Firewallregeln ständig an veränderte Anforderungen angepasst werden.



**NESEC**

Gesellschaft für angewandte Netzwerksicherheit mbH

NESEC Gesellschaft für angewandte Netzwerksicherheit mbH ist spezialisierter Anbieter von Netzwerksicherheitslösungen. Zu unserem Portfolio gehört die komplette Erstellung von Sicherheitskonzepten und die umfassende Beratung unserer Kunden ebenso wie die Installation und Konfiguration der Systeme.

Selbstverständlich sind wir auch in der Lage, Ihre Systeme vollständig zu administrieren und 24 Stunden, 7 Tage pro Woche zu überwachen.

NESEC wurde im Mai 2002 als herstellerunabhängiges Systemhaus in Freising bei München gegründet und betreibt ein eigenes, gehostetes Rechenzentrum zur Überwachung der Kundenfirewalls und Sicherheitssysteme.

Mit der Fokussierung auf Lösungen für Wachstumsmärkte in der Informationstechnologie sind sachkundige Beratung und Betreuungsqualität für NESEC handlungsleitend und Maßstab der Kundenorientierung.

Das Produktportfolio der NESEC deckt alle Bereiche der Netzwerk- und Internetsicherheit ab und ist sorgfältig auf Ihre Bedürfnisse abgestimmt. Sie erhalten individuell zusammengestellt und flexibel angepasst die jeweils modernsten Lösungen im Markt aus einer Hand.

The logo for NESEC consists of the letters 'NESEC' in a bold, sans-serif font. The 'NE' is blue and the 'SEC' is red.

Gesellschaft für angewandte Netzwerksicherheit mbH

---

NESEC Gesellschaft für angewandte  
Netzwerksicherheit mbH  
Angermaierstrasse 53 · 85356 Freising  
Tel.: 0 81 61 - 23 18 92 · Fax: 0 81 61 - 6 68 34  
welcome@nsec.de · www.nsec.de

Vertriebsbüro München  
Lichtenbergstrasse 8  
85748 Garching  
Tel.: 089 - 54 84 - 21 30  
Fax: 089 - 54 84 - 21 39

Vertriebsbüro Regensburg  
Reichsstrasse 15a  
93055 Regensburg  
Tel.: 09 41 - 2 90 75 55  
Fax: 09 41 - 2 90 75 56