

Informationssicherheit

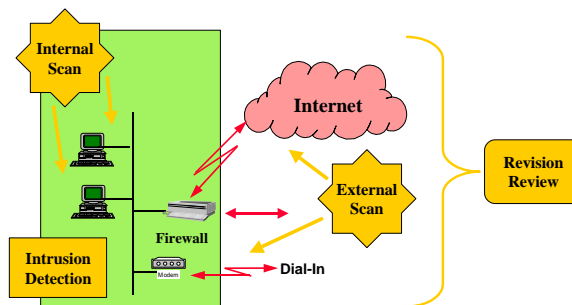
Security-Audits: Überprüfung von Schutzmaßnahmen

So dynamisch, wie die Technik im Bereich der Rechner- und Netztechnologie voranschreitet, können auch Sicherheitsmaßnahmen nie von statischer Natur sein. Neu hinzukommende Anwendungen müssen genauso beachtet werden wie die korrekte Einhaltung der getroffenen Schutzmaßnahmen. Hierzu sind in regelmäßigen Abständen oder bei Bedarf Überprüfungen vorzunehmen.

Dabei sind die Gefahren vielfältig: aus dem Internet gelten die Angriffe in erster Linie den öffentlich erreichbaren Servern und führen zum Verlust von Daten, zum Diebstahl vertraulicher Informationen oder zu unkalkulierbaren Image-Schäden. Frei erhältliche, einfach zu bedienende Tools machen es selbst Unkundigen leicht, bekannte Schwachstellen auszunutzen. Auch über Remote-Access Anbindungen für Heimarbeitsplätze oder unerlaubt betriebene Modems finden Hacker Zugang zu Unternehmensnetzen.

Bedrohungen kommen aber auch aus dem Innenbereich. Unzufriedene Mitarbeiter oder Partner-Firmen haben bereits Zugang zu Netzwerken hinter den Schutzsystemen. Aus der Sicht einer mehrstufigen Sicherheitslösung sind daher auch die lokalen Systeme im Intranet gut abzusichern und zu überwachen. Unix-Hosts sind hier ebenso betroffen wie Windows-Server oder Arbeitsplatzrechner. Mail, Web, Application- und Datenbankserver können gleichermaßen Ziel von Attacken sein wie IP- oder Network-Netze.

Zur Umsetzung der notwendigen Prüfungsszenarien bieten wir Ihnen als unabhängiges Beratungshaus die Durchführung von gut aufeinander abgestimmten **Sicherheitsprüfungen** an. Mit der Verwendung aktueller Testwerkzeuge stellen wir sicher, daß nicht nur altbekannte, sondern nachgewiesenermaßen auch aktuelle Sicherheitslücken berücksichtigt werden. In einem weitergehenden **Security-Review** untersuchen wir auch Netzpläne, Konfigurationen, Dokumentation und die Sicherheitsorganisation auf verborgene Schwächen.



Manuelle **Penetrationstests** zeigen auf, wie weit ein potentieller Angreifer in Anwendungen oder interne Netzbereiche eindringen kann. Besondere Bedrohungen unterliegt jeglicher Internet-Datenverkehr und sollte deshalb durch spezielle Content- (Mail, Web) und Application-Tests (Web- und Web-Application-Server) auf Schwachstellen überprüft werden.

Die GAI NetConsult verfügt über ein großes Erfahrungspotential bei der Umsetzung aller Phasen des Security Life Cycle. Insbesondere durch unsere herstellerneutrale Beraterstätigkeit bei der Auswahl von Schutzsystemen (Firewall, Remote-Access-Server, Kryptosysteme usw.) und Überwachungs-Tools haben wir einen profunden Überblick über Stärken und Schwächen der angebotenen Lösungen gewonnen. Mit unserer Toolbox bieten wir Ihnen verschiedene Varianten zur Überprüfung Ihrer Schutzmaßnahmen an. Die Tests werden über das Internet oder vor Ort durchgeführt, jeweils unter Berücksichtigung der besonderen Bedingungen des Produktiv- oder Test-Betriebs.

