

# White Paper

Innovative Technologie für maximale Netzwerksicherheit

## Proaktives Netzwerkmonitoring

### Stand der Technik

Im Bereich IT-Security vollzieht sich aktuell ein Technologiewechsel. Während sich in der Vergangenheit Angriffe auf die Ebene der Netzwerkinfrastruktur konzentrierten, adressieren Angreifer heute vor allem die darüberliegenden Ebenen der Applikationen. Neben zunehmenden asymmetrischen Gefahren durch gezielte Angriffe und Manipulationen generieren auch das permanent steigende Datenaufkommen und die Integration neuer Technologien (z.B. VoIP) einen steten Bedarf an Informationen über den Status, die Qualität und die Verfügbarkeit von Netzwerkservices.

Dessen ungeachtet gehören aktuell lediglich paket- bzw. regelbasierte Firewallsysteme zur Grundausstattung vieler Netzwerke. Da präventive Maßnahmen zur Verbesserung der Anwendungssicherheit immer komplex und mit einzelnen Systemen nicht mehr realisierbar sind, werden sie häufig vernachlässigt. So werden zur Netzwerkanalyse, wenn überhaupt, häufig lediglich kommunikationsbasierte Diagnosewerkzeuge eingesetzt, die den Datenverkehr protokollieren und analysieren. Die Aggregation

der Daten und die Einleitung adäquater Schutz- bzw. Abwehrmaßnahmen bleiben regelmäßig Aufgaben der Administratoren.

Intrusion Detection-Systeme liefern nur Informationen über das Netzwerkverhalten bzw. die Inhalte der Verkehrsströme am jeweiligen Standort. Gleichzeitig versuchen sie, aus dem Netzwerkverkehr Angriffsmuster zu erkennen. Diese Technologie beschränkt sich zwangsläufig auf die Informationen der jeweils untersuchten Protokollschichten und hat in der Regel keinen festen Bezug zur Netzwerkstruktur bzw. zum Kontext der Organisation. Weitergehende Informationen, die zur kontextbezogenen Analyse der erhobenen Daten notwendig sind, stehen nicht zur Verfügung. Diese Informationen müssen parallel erhoben, bereitgestellt und zur Interpretation der Messergebnisse herangezogen werden. Die Koordination dieser parallelen Prozesse, die Begutachtung der Ergebnisse, das Erkennen von Trends sowie die Einleitung reaktiver Maßnahmen bleibt letztlich qualifiziertem Fachpersonal vorbehalten. Belastbare Prognosen mit derartigen Systemen sind nicht möglich.

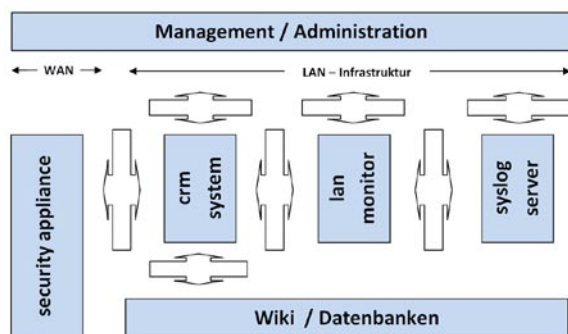
## Pro-Mon-Technologie schafft Abhilfe

Proaktives Monitoring basiert auf der Kombination kontinuierlicher agenten- und netzwerkbasierter Analysen mit kontext- und szenarienbasiertem Expertenwissen. Damit lassen sich kritische Systemzustände in IP-Netzwerken bereits in der Phase der Entstehung identifizieren und automatisiert geeignete Präventiv- bzw. Gegenmaßnahmen einleiten. Diese Funktionalität, die in verschiedensten Netzwerkkombinationen genutzt werden kann, ist ein wesentliches Alleinstellungsmerkmal der Pro-Mon-Systeme

Pro-Mon geht damit weit über die Ansätze konventioneller Lösungen hinaus. Bezogen auf den jeweiligen netzwerktechnischen und administrativen Kontext werden nicht nur Daten erhoben, Gefährdungen erkannt und Handlungsempfehlungen abgeleitet. Vielmehr kann ein voll ausgebautes System automatisiert und angemessen auf dynamische Angriffssituationen reagieren. Die Kombination und Verschmelzung der an beliebigen Stellen erhobenen Netzwerk-Reportingdaten mit den Informationen externer Quellen, der Abgleich mit den Helpdesk-Informationen sowie die Ableitung von Handlungsempfehlungen setzen Maßstäbe für eine neue Qualität des Monitoring.

## Maßgeschneidert für Netzwerke

Pro-Mon Systeme sind funktional nicht standardisiert sondern in jedem Fall an vorhandene Infrastrukturen und administrative Kompetenzen zu adaptieren. Dabei ist auf Basis der konkreten Anforderungsprofile der Funktionsumfang individuell wählbar. Eine Übersicht verfügbarer Funktionsmodule liefert das Prinzipschaltbild.



Die Implementation eines Pro-Mon-Systems erfolgt regelmäßig in mehreren Stufen. Im ersten Schritt, der Netzwerk- und Risikoanalyse, werden strukturelle sowie technische Parameter und Defizite erfasst und bewertet. Aus den Ergebnissen leiten die Sicherheitsexperten dann das Sicherheitskonzept ab. Im Zuge des Systemdesigns werden im Anschluss notwendige Funktionsmodule gemäß der kunden-, d.h. netzwerkspezifischen Anforderungen kombiniert und schlussendlich konfiguriert.

Wesentlichen Einfluss auf die Dauer und den nachhaltigen Erfolg jeder Pro-Mon Implementation hat neben dem Projektmanagement vor allem das Know-how der Administratoren und Netzwerkmanager. Daher sollten bereits im Vorfeld der notwendigen Schulungsbedarf erhoben und ggf. detaillierte Qualifikationspläne aufgestellt werden.

## Kundennutzen

Automatisierte, expertengestützte, proaktive Reaktionen auf detektierte Gefährdungs- bzw. Bedrohungslagen erhöhen die Sicherheit und minimieren Ausfallrisiken.

Die Entscheidung zur Einführung eines Pro-Mon Systems sollte grundsätzlich unter Berücksichtigung der personellen und technischen Ressourcen erfolgen. Während die Verantwortlichen kleiner IT-Infrastrukturen oft besser damit beraten sind, das komplette Netzwerk- und Servicemanagement extern realisieren zu lassen, ist die Einführung von Monitoring-Technologien für Administratoren komplexer Netzwerke auf Dauer zwingend.

Letztlich ist die Einführung transparenter und reproduzierbarer Überwachungstechnologien die Basis jedes qualifizierten Netzwerkmanagements. Regelmäßig setzen Qualitätsmanagementsysteme wie ISO oder Servicemanagementzertifizierungen wie ITIL derartige Systeme voraus.