

# Network Intrusion Detection

## Lösungsbeschreibung - Kurzfassung

**Intrusion Detection: Proaktive Security, Angriffserkennung und Verhinderung in Ergänzung zu einer Firewall**

### KURZABRISS

Ein Intrusion Detection System ersetzt nicht etwa die Firewall sondern stellt eine sinnvolle Ergänzung dar. Man kann sich hier einer Analogie zur Gebäudesicherung bedienen: Der Zugang zum Internet (oder auch zu einem anderen Netz ausserhalb des eignen LAN's) ist ein Eingang. Den verschliesst man üblicherweise mit einer Tür in der sich auch ein vernünftig ausgelegtes Schloss befinden sollte. Ein Intrusion Detection System (IDS) an dieser Stelle ist die Alarmanlage - also eine Möglichkeit Aktivitäten zu erkennen die auf einen Einbruch hindeuten.

Weiterhin kann man ein IDS nutzen um Statistiken zu erstellen - welche Angriffe werden auf das Netz gemacht, welchen Nutzen hat also die Firewall. Das kann zur Plausibilisierung einer Security Infrastruktur dienen, zum Beispiel im Rahmen einer Betriebsinternen Revision.

Das System selber besteht aus zwei Komponenten:

1. Den sogenannten Sensoren. Das sind Software Instanzen die auf folgenden Hardware/OS läuft: Sun Solaris, NT, Nokia. Die Sensoren können - abhängig davon welche Systeme man schützen oder welche Angriffe man reporten möchte - an verschiedenen Stellen im Netzwerk positioniert werden.
2. Dem Workgroup Server, der die Ereignisse der Sensoren sammelt und auf den man mit der GUI (Graphical User Interface) zugreift um das System zu konfigurieren, administrieren und Ergebnisse abzufragen.

Der wesentliche Part eines solchen Systems ist aber ein sinnvolles Betriebskonzept und eine IDS Policy. Erst mit der Anpassung an die Kundensituation und den Kundenbedarf wird aus dem System eine handhabbare Lösung.

Die Lösung von choin! besteht dementsprechen aus

- einem Lösungskonzept mit den Themen: Einbindung in das Netzwerk, Admin Prozesse bei Meldung eines Einbruchs.

- dem System (wie oben beschrieben, Sensoren und Groupmanager)
- Wartungsverträge zum System
- pro Sensor und dem Workgroupserver je einer dedizierten Hardware auf dem diese Software läuft
- Erstellung einer IDS Policy (was soll erkannt und gemeldet werden, automatische Reaktionen des
- IDS bei Angriffserkennung wie z.B. Connection Reset)
- Dokumentation der Lösung.

Die Lösung kann und wird auch im Rahmen der Managed Security Lösung eingesetzt. Auf Wunsch des Kunden können wir also die Lösung auch als reinen Service - unabhängig vom Standort (Customer Side, Datacenter Side) anbieten.

Verwandte Themen sind Host Intrusion Detection, Security Scanner.

### VORTEILE

- Schutzmassnahmen wie Firewalls können das Riskiko eines Einbruchs zwar reduzieren, aber nie völlig eliminieren - ein IDS erhöht den Sicherheitslevel und gleicht Schwächen oder eine eventuell notwendige tolerante Firewall Policy aus.
- Angriffe die nicht von der Firewall geblockt werden, werden nicht erst durch einen Ausfall von Systemen oder bei einer Überprüfung und Auswertung des Firewall Logs erkannt, sondern im Moment des Angriffs. Dadurch lassen sich mögliche Schädigungen vermeiden oder reduzieren.
- Bei Positionierung eines Sensors vor der Firewall können sämtliche Angriffe gescant, statistisch erfasst werden und somit zur Plausibilisierung oder im Rahmen einer Revision sehr hilfreich sein.
- Über ein IDS lassen sich Angriffe automatisiert (z.B. connection reset oder Rekonfiguartion der Firewall) abwehren. Das ist allerdings aufgrund der nicht möglichen 100% Erkennung umstritten und erfordert viel Arbeit bei der Konfiguartion der IDS Policy.

#### **Anschrift**

choin! GmbH  
Weinheimer Str. 68  
D-68309 Mannheim

#### **Kontakt**

Tel. +49 (0) 621-72 84 85 - 1000  
Fax +49 (0) 621-72 84 85 - 1060  
Email: [verkauf@choin.net](mailto:verkauf@choin.net)  
URL [www.choin.net](http://www.choin.net)

#### **Bankverbindung**

Volksbank Weinheim  
Kto. 39 56 504  
BLZ 670 923 00

Sitz der Firma: Heppenheim

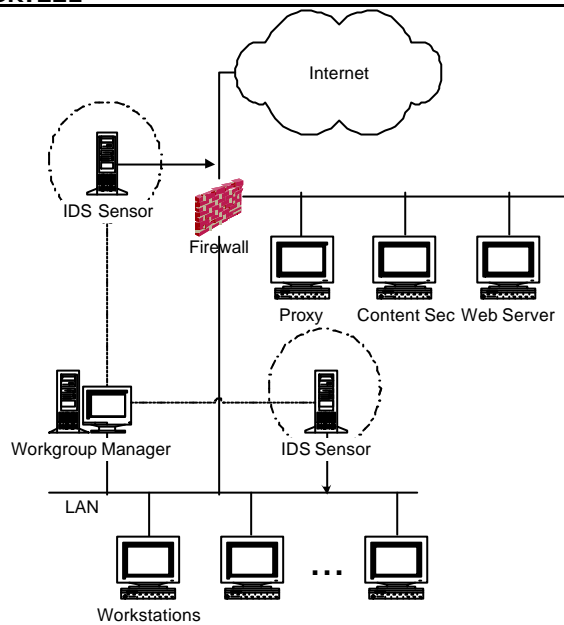
Handelsregister: Bensem HRB 25 455  
Geschäftsführer: Boris Wetzel

Ust.IdNr.: DE222 588 770

## ANFORDERUNGEN

Zielmarkt sind mittlere und grosse Unternehmen, bevor ein Gesamtangebot erstellt wird ist - gerade bei Einbindung in eine bestehende Infrastruktur - ein Konzept mit oben genannten Inhalten unerlässlich.

## SKIZZE



## KONTAKTINFO

Das Aufsetzen einer Lösung dieser Art für den Kunden resultiert immer in einem choin!-Projekt.

Sollten Sie weitere Fragen zu diesem Thema haben, so wenden Sie sich vertrauensvoll an unser Vertrieb.

### **Anschrift**

choin! GmbH  
Weinheimer Str. 68  
D-68309 Mannheim

### **Kontakt**

Tel. +49 (0) 621-72 84 85 - 1000  
Fax +49 (0) 621-72 84 85 - 1060  
Email: [verkauf@choin.net](mailto:verkauf@choin.net)  
URL [www.choin.net](http://www.choin.net)

### **Bankverbindung**

Volksbank Weinheim  
Kto. 39 56 504  
BLZ 670 923 00

Sitz der Firma: Heppenheim

Handelsregister: Bensheim HRB 25 455  
Geschäftsführer: Boris Wetzel  
Karl H. Michalik  
Ust.IdNr.: DE222 588 770