

## Neue Intrusion-Prevention-Technologie verhindert auch unbekannte Angriffe

### cirosec bietet seinen Kunden ab sofort das Produkt ActiveScout von ForeScout an

HEILBRONN, 28. April 2003 – Die cirosec GmbH bietet seinen Kunden ab sofort das neue Produkt ActiveScout von ForeScout an. Dieses Intrusion-Prevention-System ist in der Lage, tatsächliche Angreifer ohne Fehlalarme zu erkennen und sie dann auszusperrern.

Herkömmliche Intrusion-Detection-Systeme (IDS) haben noch immer das Problem der vielen Falsch-Positiv-Alarme. Sie erkennen Attacken meist erst dann, wenn es bereits zu spät ist und bieten somit keinen aktiven Schutz. Die Technologie von ForeScout hat einen anderen Ansatz. Sie kennt das Vorgehen von Hackern und macht sich dieses zunutze.

Normalerweise startet ein Angriff, indem ein Angreifer mit verschiedenen Methoden versucht, Informationen über das Unternehmensnetzwerk zu sammeln. Im nächsten Schritt werden diese Informationen genutzt, um gezielte Angriffe zu starten.

ForeScout erkennt im Gegensatz zu herkömmlichen IDS-Systemen nicht die Attacken, sondern dieses angreifertypische Verhalten. Wird dieses beobachtet, werden dem vermeintlichen Angreifer nicht existente Schwachstellen, wie offene Ports oder Benutzernamen und Passwörter vorgetäuscht. Nun beobachtet ActiveScout, wie der vermeintliche Angreifer auf diese Falsch-Informationen reagiert. Versucht er sie auszunutzen, ist klar, dass es sich auf jeden Fall um einen Angriff handelt und nicht um einen einfachen Scan. Der Hacker wird daraufhin blockiert und ausgesperrt.

ActiveScout blockiert den Angriff auf zwei verschiedene Methoden. Zum einen durch automatisches Einfügen einer temporären Regel auf der Firewall und zum anderen durch so genannte TCP-Resets, bei denen die Angreifer-Session sofort abgebrochen wird. Versucht der Angreifer von anderen IP-Adressen aus, die vorgetäuschten Schwachstellen auszunutzen, wird er sofort wieder ausgesperrt, da ActiveScout ihn an den Falsch-Informationen erkennt.

Rainer M. Richter, Vice President EMEA von ForeScout und ehemaliger General Manager von Nokia Internet Communications ist von der Technologie seines Unternehmens überzeugt. „Dies ist die weltweit erste Technologie, die unabhängig von der verwendeten Angriffstechnik den Angreifer an seiner Intention erkennt und aussperrt, ohne Falsch-Positiv-Alarme zu geben.“

„ForeScout geht im Vergleich zu anderen Herstellern einen völlig neuen Weg um Intrusion Prevention zu realisieren. Bis jetzt war jeder unserer Kunden, der die Technologie einmal getestet hat, davon begeistert“, so Stefan Strobel, Geschäftsführer von cirosec.