

LAN-Security Check

Der Net4You LAN Security Check prüft automatisch die im Netzwerk installierten Systeme und Dienste und simuliert in kontrollierter Weise häufig anzutreffende Einbruchsverfahren oder Angriffsszenarien. Mit der Überprüfung Ihres LANs tun Sie einen wichtigen Schritt in Richtung Netzwerksicherheit!



Sicherheitslücken?

Mit dem Net4You LAN Security-Check werden für IT-Administratoren folgende Fragen beantwortet:

- Welche Sicherheitslücken sind für Hacker ersichtlich?
- Wie können sie diese Lücken ausnutzen?

Der LAN Security Check deckt nicht nur einfach Schwachstellen auf, sondern bietet zudem einen systematischen Einblick in die Ursachen, die zur Entstehung dieser Schwachstellen im System führten. Wird durch den LAN Security Check beispielsweise ein Kennwort auf einem System „geknackt“, wird es anschließend auch auf den anderen Systemen getestet. Das Ergebnis ist eine gründlichere Analyse und eine exaktere Darstellung der Schwachstellen.

Die Analyse kann grob in einen Aktiven und einen Passiven Part (Sniffer) unterteilt werden. Für den Passiven Teil sind folgende

Voraussetzungen zwingend erforderlich:

- Pro LAN Segment (Switch) muss ein 100mbit Managerport zur Verfügung stehen, auf dem der gesamte Datenverkehr mitprotokolliert werden kann.
- LWL Verbindungen teilen das Netzwerk in Segmente. Der passive Check muss daher „auf jeder Seite“ durchgeführt werden.
- LAN interne Router segmentieren das Netzwerk ebenfalls. Auch hier muss der passive Check auf „jeder Seite“ durchgeführt werden.

Passiver Check

Beim Passiven Check wird der gesamte anfallende Datenverkehr im jeweiligen Segment mitprotokolliert und auf zuvor definierte Parameter untersucht. So können beispielsweise Programme wie ICQ, File-Sharingtools, Sniffer, Passwort-Scanner gesucht und auch gefunden werden. Weiters wird die Auslastung des Netzwerkes detailliert festgehalten. Damit ist es möglich, Engstellen im Netzwerk frühzeitig zu erkennen, bzw. nicht benötigte Dienste zu lokalisieren.

Aktiver Check

Ein aktives Scannen von definierten IP Bereichen mit Protokollierung nachfolgender Punkte:

- Feststellung des Betriebssystems und der Version (sofern möglich)
- Probe der Zielrechner auf Standardpasswörter/Laufwerksfreigaben
- Protokollieren der aktiven Ports mit Auswertung der vermuteten Dienste
- Probe der Zielrechner auf bereits installierte Trojaner.

Der aktive und passive Teil ergeben gemeinsam einen sehr detaillierten Überblick über die aktuelle Situation in Ihrem Netzwerk. Eine Besprechung der Ergebnisse des LAN Security Checks und der daraus resultierenden Empfehlungen gibt Ihnen die Möglichkeit, entsprechende Maßnahmen zur Absicherung Ihres Netzwerkes zu ergreifen.