IT-Sicherheits-Scans für Server und Subnetze

Um größtmögliche Netz- und Datensicherheit im Intranet der Ruhr-Universität zu erreichen, müssen die angeschlossenen Endgeräte und Server regelmäßig mit den aktuellen Sicherheitskorrekturen versorgt und die darauf installierten Dienste gegen mögliche Schwachstellen abgesichert werden. Leider reicht es häufig nicht hin, die aktuellen Betriebssystem-Updates einzuspielen. Immer wieder treten Schwachstellen in Applikationen auf, für die es keine Sicherheitskorrekturen gibt, oder es treten unbeabsichtigt Konfigurationsfehler auf.
Die Stabsstelle IT-Sicherheit bietet die Überprüfung von Windows-, Linux- oder Unix-Servern auf bekannte Sicherheitslücken und Schwachstellen an. Als Ergebnis eines solchen Scans wird ein Protokoll erzeugt, das potentielle Schwachstellen des Servers auflistet und Empfehlungen für die erforderlichen Maßnahmen gibt.
Die Überprüfungen werden mit dem bekannten Netzwerk- und Sicherheitsscanner Nessus in der erweiterten professionellen Version durchgeführt. Dies garantiert den Zugriff auf die neuesten aktuellen Sicherheitstests.

Was wird überprüft

Ein Standard-Scan beinhaltet Tests auf bekannte Sicherheitslücken in den Diensten, die auf dem Server laufen. Ein erweiterter Scan beinhaltet zusätzlich einen Test auf Betriebssystemschwachstellen.

Wer kann einen Sicherheitsscan veranlassen

Die Beauftragung eines Sicherheitsscans erfolgt ausschließlich durch Netzbetreuer, die dem Network Operation Center (NOC) als Ansprechpartner für ein IP-Subnetz der Ruhr-Universität Bochum benannt worden sind. Die IP-Nummer des zu testenden Servers muss zu dem IP-Subnetz der Ruhr-Universität gehören, für das der Netzbetreuer zuständig ist. Das Ergebnis des Scans erhält der Netzbetreuer in Form einer HTML-Datei bzw. als Papierausdruck.
Bei Interesse können sich Netzbetreuer per E-Mail oder telefonisch an die Stabsstelle IT-Sicherheit wenden.

Brigitte Wojcieszynski
Tel.: 0234 / 32-23409
Sekretariat: 0234 / 32-24001
itsb@rub.de