Der Netzwerkprüfer

Das DFN-CERT Portal (Teil 3)

Text: **Gerti Foest** (DFN-Verein), **Tilmann Haak** (DFN-Cert Services GmbH), **Jochen Schönfelder** (DFN-Cert Services GmbH)

Foto: © Justin Allfree - istockphoto

Wie sieht das Netzwerk einer Einrichtung eigentlich von außen aus? Was sieht zum Beispiel ein potentieller Angreifer und was kann er über das lokale Netz herausfinden? Deckt sich das, was nach außen sichtbar sein soll mit dem, was nach außen sichtbar ist und sind tatsächlich nur die Dienste von außen erreichbar, die frei verfügbar sein sollen oder können auch Dienste erreicht werden, die eigentlich nur lokal genutzt werden sollten?

Der Netzwerkprüfer gibt Sicherheitsverantwortlichen und Firewall-Administratoren die Möglichkeit, von außen zu testen, ob sich die tatsächliche Erreichbarkeit der lokalen Systeme mit der gewünschten Erreichbarkeit deckt, indem sie einen Scan von Netzbereichen oder einzelnen IP-Adressen in Auftrag geben können. Im Gegensatz zu den automatischen Warnmeldungen, die in ihrer Natur reaktiv sind, ist der Netzwerkprüfer proaktiv. Er zeigt mögliche Sicherheitslücken auf, bevor etwas passiert ist. Anhand der Ergebnisse eines Scans durch den Netzwerkprüfer haben die Verantwortlichen die Möglichkeit, die Zu-

gänge zu ihrem lokalen Netz neu zu konfigurieren und damit die Wahrscheinlichkeit von Sicherheitsvorfällen zu verringern.

Der dritte Dienst im DFN-CERT Portal

Der Netzwerkprüfer ist der dritte Dienst, der DFN-Anwendern neben den automatischen Warnmeldungen (DFN-Mitteilungen Heft 76, S.44 ff.) und den Informationen zu Schwachstellen (DFN-Mitteilungen Heft 77, S.40 ff.) über das DFN-CERT Portal zur Verfügung steht.

Wie bei allen Diensten im DFN-CERT Portal ist der Zugriff auf den Netzwerkprüfer zertifikatgesteuert. Nur „handlungsberechtigte Personen“ (HP) können einen Scan-Auftrag für ihre Einrichtung im DFN-CERT Portal absetzen. Eine handlungsberechtigte Person wird von einer Einrichtung schriftlich für die Dienste im DFN-CERT Portal als verantwortlicher Ansprechpartner benannt. Nachdem das Formular für diese Person eingegangen ist, wird deren Zertifikat für die Nutzung freigeschaltet. Vor dem Absetzen eines Scan-Auftrags muss die HP im Portal noch einmal bestätigen, dass sie berechtigt ist, den Scan für diesen Netzbereich der Einrichtung durchzuführen.

Für einen Auftrag müssen der IP-Bereich, die Art des Scans und eine E-Mailadresse angegeben werden (Abbildung 1). Da Beginn und Abschluss eines Auftrags von der Größe des zu scannenden Bereichs, den Gegebenheiten des Netzwerks und der Auslastung des Dienstes durch weitere Aufträge abhängen, können sie nicht im Voraus berechnet werden. Deshalb wird an die angegebene E-Mailadresse jeweils zu Beginn und bei Abschluss eines Scans eine Benachrichtigung geschickt.

In Abbildung 2 ist ein Scan-Ergebnis zu sehen. Die aktiven IP-Adressen werden tabellarisch aufgelistet, ein Klick auf eine der IP-Adressen zeigt weitere Details und gibt die Möglichkeit, einen gezielten Scan einer einzelnen Adresse direkt zu beauftragen. Es stehen zwei verschiedene Scan-Arten zur Verfügung: Standard- und Tiefenscan. Der Standardscan liefert zügig einen guten Überblick, indem zur Zeit die ca. 2.500 wichtigsten TCP- und UDP-Ports gescannt werden. Dieses Vorgehen deckt sich auch mit dem Verhalten der meisten Angreifer. Alle möglichen Ports zu prüfen, würde deutlich mehr Zeit erfordern. Der Tiefenscan führt zusätzlich eine Diensterkennung auf den gefundenen offenen Ports aus und listet diese so detailliert wie möglich auf (Abbildung 3).

Abb. 1: Vorbereiten eines Scan-Auftrags

Der Blick hinter die Kulissen

Um die Scan-Aufträge abzuarbeiten, wird im Hintergrund ein regelbasiertes Scansystem eingesetzt. In einem mehrstufigen Verfahren wird zunächst überprüft, welche IP-Adressen innerhalb des Scan-Auftrags aktiv sind. Anschließend werden die notwendigen Scans durchgeführt. Hierbei muss an mehreren Stellen vereinfacht werden, da ein kompletter UDP-Portscan abhängig von der Firewallkonfiguration einer Einrichtung mehrere Tage dauern könnte, selbst wenn nur eine IP-Adresse gescannt wird. Bei der Auswahl der zu scannenden Ports und der verwendeten Techniken wird versucht, dem Verhalten eines potentiellen Angreifers möglichst nahe zu kommen.

Die benötigten Paketraten und Datenmengen eines Scans sind ein Kompromiss zwischen der Scan-Geschwindigkeit und der Last, die auf den lokalen System- und Netzkomponenten entsteht. Das Ergebnis eines Standardscans für ein Class-C Netz kann somit in der Regel innerhalb von wenigen Minuten geliefert werden.

Stand des Dienstes

Der Netzwerkprüfer befindet sich derzeit im Testbetrieb. Gemeinsam mit den teilnehmenden Einrichtungen wird erprobt, wie er noch besser auf die Anforderungen der Anwender zugeschnitten werden kann. Die Rückmeldungen fließen direkt in die Entwicklung mit Blick auf den Regelbetrieb ein.

Die Überführung des Netzwerkprüfers in den Regelbetrieb ist in einem Netz von der Größe des Deutschen Forschungsnetzes eine nicht geringe Herausforderung. Schon der Scan eines Class-B Netzes benötigt mehrere Stunden. Treffen mehrere solcher Scan-Aufträge gleichzeitig ein, wird die Bearbeitung voraussichtlich nicht an einem Tag abgeschlossen werden können. Aktuell wird durch Integration mehrerer Scan-Knoten daran gearbeitet, dass auch mehrere parallele Scans unterschied-

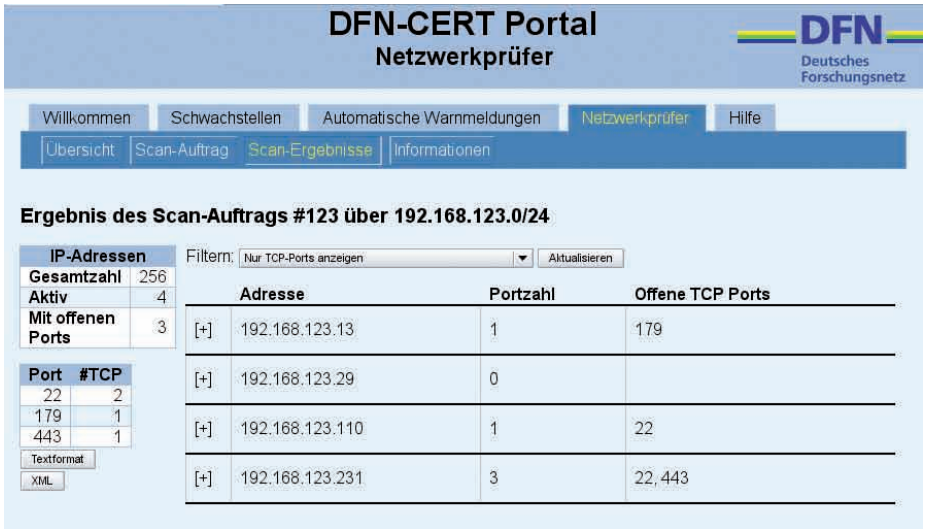

Abb. 2: Ergebnis eines Standardscans über einen IP-Bereich

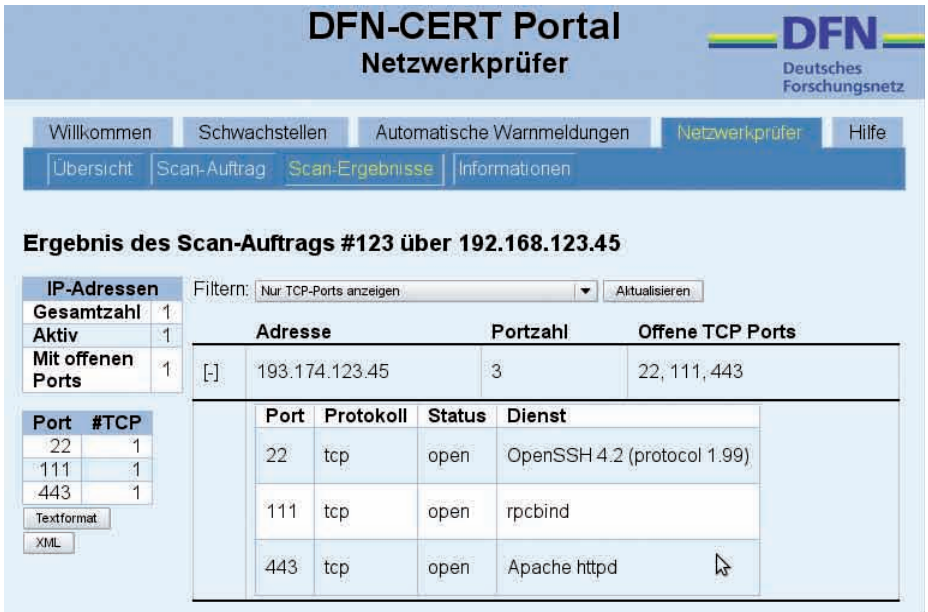

Abb. 3: Ergebnis eines Tiefenscans mit Diensterkennung

licher Einrichtungen in vertretbarer Zeit abgeschlossen werden können.

Ausblick

Das Scansystem wird laufend weiter entwickelt, um zusätzliche Informationen zu erfassen und auszuwerten. So wird das System demnächst z. B. in der Lage sein, kritische Sicherheitslücken in den Ergebnissen zu kennzeichnen. In Vorbereitung sind außerdem Konfigurationsmöglichkeiten für regelmäßig durchzuführende Scans. Deren Ergebnisse zeigen nicht nur den aktuellen Zustand, sondern vergleichen ihn zusätzlich mit vorangegangenen Scans. So können die Anwender gezielt auf (gewollte oder ungewollte) Veränderungen in ihren Systemen hingewiesen werden.

Nach Abschluss des Testbetriebs zur Betriebstagung im Oktober 2010 wird der Netzwerkprüfer dann allen am DFN-CERT teilnehmenden Einrichtungen zur Verfügung stehen. Für die weitere Zukunft ist geplant, vom Netzwerkprüfer gefundene Dienste in Bezug auf bekannte Schwachstellen zu analysieren und eine Verbindung zu den Informationen zu Schwachstellen herzustellen. Damit können die Anwender noch gezielter bei der Entdeckung und Beseitigung von Betriebsrisiken unterstützt werden.

Zusammenfassung

Umfangreiches Wissen über das Netzwerk einer Einrichtung ist die Basis für eine erfolgreiche Sicherheitsstrategie. Nur wenn Administratoren auch die Außenansicht ihres lokalen Netzwerks kennen, können sie Fehlkonfigurationen erkennen und entsprechend handeln, bevor jemand Unbefugtes es tut. Durch den Netzwerkprüfer steht nun auch ein proaktiver Dienst im DFN-CERT Portal zur Verfügung, der die DFN-Anwender bei der Sicherung ihrer Netze und Kommunikationswege unterstützt.

Info

Sie erreichen das DFN-CERT Portal unter https://portal.cert.dfn.de/.

Weitere Informationen und eine ausführliche Nutzungsanleitung finden Sie unter https://www.cert.dfn.de/nwp.

Für Fragen und Anregungen zur Nutzung des Portals schicken Sie bitte eine E-Mail an: cert@dfn.de. ◆