Hintergrundwissen:

Firewalls, Segmentierung und Verinselung

Zum Thema Verinselung
Zu den Firewalls

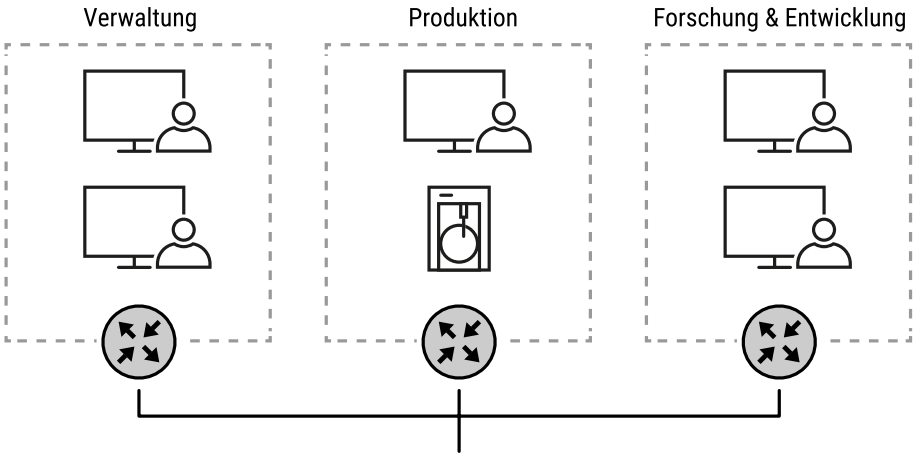
Eine verbreitete Technik zur Verbesserung der Sicherheit in Unternehmensnetzwerken ist, diese nach Abteilungen in kleinere Segmente zu untergliedern. Die Kommunikation zwischen diesen Subnetzen wird von Firewallroutern überwacht, gesteuert und protokolliert. Angreifer und Schadsoftware, denen es gelingt, in eines der Subnetze einzudringen, werden von Paketfiltern an einer weiteren Ausbreitung gehindert. Eine Maßnahme zur weiteren Steigerung der Sicherheit ist das gezielte Isolieren einzelner Systeme und Funktionseinheiten in einem jeweils eigenen Netzwerksegment. So lassen sich auch besonders gefährdete Geräte effektiv schützen.

Segmentierung: Unterteilung in sichere Subnetze

Das Internetprotokoll (IP) macht es möglich, Daten über Netzwerkgrenzen hinweg auszutauschen. Die in IP-Paketen gekapselten Informationen werden über verschiedene Router hinweg zu ihrem Ziel geleitet.

Diese Routing-Eigenschaft machen sich Netzwerkadministratoren zu Nutze, um Unternehmensnetze in miteinander verbundene Subnetze zu unterteilen. Die Rechner der Verwaltung werden dem Subnetz der Verwaltung zugewiesen, auch Maschinen in der Produktion erhalten ein eigenes Netzwerksegment, genauso wie die Arbeitscomputer in der Abteilung Forschung & Entwicklung.

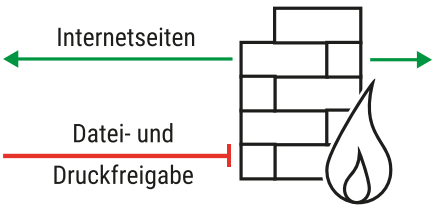
Jedes dieser Netzsegmente wird über einen Router an das umgebende Unternehmensnetz angebunden. Jegliche Kommunikation zwischen den Subnetzen wird über die Router geleitet.



Paketfilter für mehr Sicherheit

Es bietet sich an, die vorbeigeleiteten Datenpakete am Router zu untersuchen und nur zulässige Datenpakete weiterzuleiten.

Es könnte etwa im Interesse der Unternehmensführung liegen, dass Mitarbeiter der Verwaltungsabteilung zwar frei auf Webseiten im Internet zugreifen können, gleichzeitig aber deren sensible Daten, wie Gehaltsabrechnungen oder Verträge, im Unternehmensnetz und Internet unzugänglich bleiben. Diese werden im Windowsnetzwerk über die Datei- und Druckerfreigabe zur Verfügung gestellt.



Ein auf dem Router installierter Paketfilter untersucht nun, ob der vorbeigeführte Netzwerkverkehr Verbindungen enthält, die von der Datei- und Druckerfreigabe verwendet werden. Das sind TCP-Verbindungen an die Ports 139 und 445. Erkennt der Paketfilter IP-Pakete, die TCP-Kommunikation mit diesen Ports enthalten, werden diese nicht weitergeleitet, sondern verworfen. Während die Datei- und Druckerfreigabe innerhalb des Subnetzes für die Verwaltung weiterhin funktioniert, kann sie die Segmentgrenzen nicht überschreiten. Auf Dateien wie Gehaltsabrechnungen kann aus anderen Netzwerksegmenten heraus also nicht zugegriffen werden.

Ein Router, der den Datenfluss auf diese Weise filtert, wird Firewall-Router oder kurz Firewall genannt.

Verinselung: Gezieltes Segmentieren einzelner Systeme

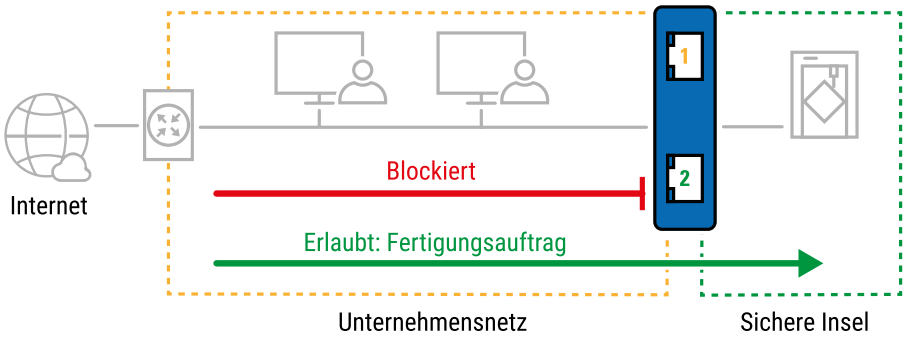
Die Firewall-Regeln für große Subnetze können schnell unübersichtlich werden. Sind sie zu großzügig ausgelegt, können Sie von Angreifern ausgenutzt werden. Sind sie zu eng gefasst, kann es zu Funktionseinschränkungen kommen. Jedes Endgerät in einem Segment ist außerdem eine mögliche Quelle unerwünschter Zugriffe.

Besonders Geräte und Systeme mit hohem Schutzbedarf - beispielsweise Werkzeugmaschinen, Medizingeräte, aber auch ältere Steuerrechner oder Rechner, mit veralteter Software - weisen mitunter bekannte, ausnutzbare Sicherheitslücken auf, die von den Regeln nicht mehr erfasst werden.

Verinselung bedeutet, diese besonders gefährdeten Systeme im Netzwerk zu identifizieren und mit Hilfe von Kleinfirewalls wie der Microwall in einem eigenen Netzwerksegment - auf einer sicheren Insel - zu isolieren. Die notwendigen Verbindungen zwischen

Systemen auf der Insel und dem umgebenden Netzwerk werden im Vorfeld erfasst und durch eine Positivliste von Regeln beschrieben. Nur ausdrücklich zugelassene Datenpakete werden weitergeleitet, alle anderen werden verworfen und bei Bedarf protokolliert. Verinselte Systeme werden so effektiv vor Angriffen durch Hacker oder Malware, sowie vor menschlichen Fehlern geschützt.

Auf diesen sicheren Inseln befinden sich nur wenige Systeme. Dadurch, dass diese durch einen eng gefassten und genau auf die jeweilige Aufgabenstellung angepassten Regelsatz geschützt werden, sorgt die Verinselung für deutlich gesteigerte Sicherheit.



Verinselung mit der Microwall ist einfach umzusetzen und steigert effektiv das Sicherheitsniveau im Unternehmensnetz. Davon profitieren insbesondere kleinere Betriebe, für die sich eine aufwändige Segmentierung nach Abteilungen nicht lohnt.

Probieren geht über Studieren!

Gerne stellen wir Ihnen für den Zeitraum von vier Wochen eine Microwall kostenfrei zur Verfügung.

Testgerät anfordern

Thomas Clever
t.clever@wut.de

Sie erreichen unsere Techniker telefonisch unter 0202/2680-110 (Mo-Fr. 8-17 Uhr)

W&T
www.WuT.de

Wir sind gerne persönlich für Sie da:

Wiesemann & Theis
GmbH
Porschestr. 12
42279 Wuppertal
Tel.: 0202/2680-110 (Mo-Fr. 8-17 Uhr)
Fax: 0202/2680-265
info@wut.de