1 Ratgeber und Praxis

Nicht nur große, sondern zunehmend auch mittlere und kleine Unternehmen sind Zielscheibe von Cyberkriminellen. Dieses Kapitel gibt IT-Verantwortlichen und Administratoren einen praxisrelevanten Überblick über wichtige Grundlagen für einen besseren Schutz ihrer IT-Infrastruktur. Es befasst sich mit den wachsenden Herausforderungen des Sicherheitsmanagements, aktuellen Bedrohungsszenarien und erfolgversprechenden Abwehrmaßnahmen.

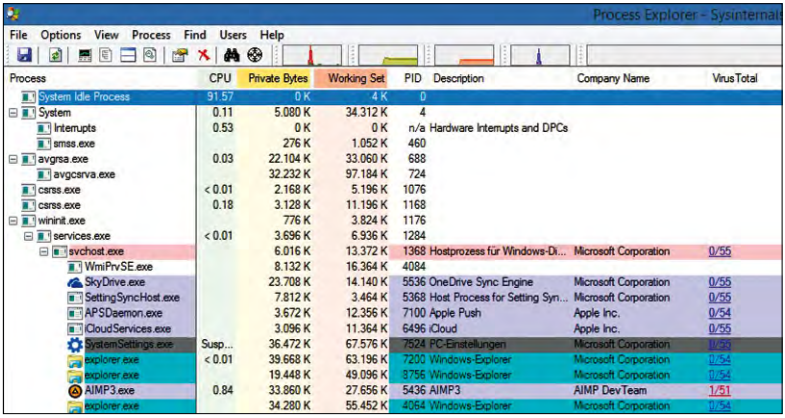
1.1 So erkennen Sie Hacker auf Servern

IT-Verantwortliche müssen Server mit speziellen Tools und Maßnahmen ständig überwachen, um Angreifer rechtzeitig zu erkennen und zu bekämpfen. Denn Hacker sind kreativ und in der Lage, die standardisierten Sicherheitsmaßnahmen eines Unternehmens auszuhebeln. Greifen Hacker das Unternehmen an, besteht grundsätzlich auch die Gefahr, dass die Server kompromittiert werden. Das passiert vor allem in kleinen Unternehmen, deren Netzwerke oft nur unzureichend vor Angriffen geschützt sind. Aber auch bei größeren Unternehmen besteht generell die Gefahr, dass sich Hacker oder Schadsoftware auf den Servern einnisten. Um Böses abzuwenden, verlassen sich viele Verantwortliche dabei auf den Virenschutz der Rechner. Dieser erkennt aber nicht alle Angreifer.

In diesem Beitrag geben wir Ihnen einige Hinweise, wie Sie verdächtigen Aktionen auf die Schliche kommen. Zunächst sollten Sie im Netzwerk ständig überprüfen, ob es Probleme bezüglich der Arbeitsstationen gibt. Wenn Netzwerke gehackt werden, dann oft über den Weg der Client-Computer. Sind Angreifer aber im Unternehmen angekommen, sind auch die Server in Gefahr. Das gilt vor allem dann, wenn zwischen dem Netzwerk mit den Client-Computern und den Servern keine Firewall positioniert ist, die den Datenverkehr Port-genau filtern kann. Wenn Hacker erst die Server im Visier haben, werden oft Bot-Schädlinge installiert, Trojaner lesen Daten aus, oder der E-Mail-Server wird als Spam-Relay missbraucht. Natürlich gibt es eine Vielzahl weiterer Angriffsmöglichkeiten, die Unternehmen vor Probleme stellen können. Wir zeigen, wie Sie diese erkennen und beheben können.

1.1.1 Server auf verdächtige Prozesse untersuchen

Wenn Server unter einer hohen Last laufen, sollten Sie im Task-Manager überprüfen, welche Prozesse gestartet sind. Prozesse, die Sie nicht erkennen, sollten Sie genauer überprüfen. Hier stehen für Serverdienste auch spezielle Tools zur Verfügung, die bei der Analyse helfen können. Vor allem wenn es um die Serverüberwachung geht, verwenden viele Administratoren den kostenlosen **Sysinternals Process Explorer** (www.tecchannel.de/2034774).



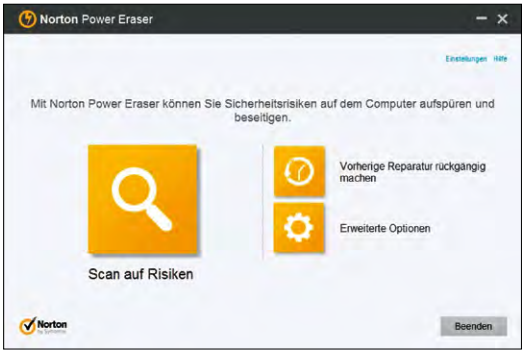
Process Explorer: Das Tool zeigt Prozesse auf Rechnern an und erlaubt eine umfassende Analyse.

Über das Kontextmenü können Sie mit Search Online direkt im Internet nach dem Prozess suchen lassen. Finden Sie einen Angreifer, dann sollten Sie diesen aber nicht sofort löschen. Prüfen Sie erst, wo er herkommt, und eliminieren Sie ihn an der Quelle. Löschen Sie nur den Prozess. Achten Sie auch auf Prozesse, die zunächst seriös klingen – die wenigsten Angreifer nennen Ihren Schädling *hack.exe*. Über das Kontextmenü von Prozessen können Sie diese mit Check Virus Total online nach Viren scannen lassen.

1.1.2 Bots und Rootkits entfernen

Besonders häufig werden Server von Bots oder Rootkits angegriffen. Diese werden erfahrungsgemäß eher selten von Standard-Viren-Scannern erkannt, sondern nur von speziellen Tools, die dafür entwickelt wurden.

Spezialaufgabe: Bot-Schädlinge entfernen Sie mit kostenlosen Tools wie Norton Power Eraser.



Wenn ein Server in Ihrem Unternehmen von einem Bot-Schädling angegriffen wurde, kann der Server über den Schädling Rechenaufgaben im Namen des Angreifers durchführen. Diese werden entweder für das Versenden von Spam-E-Mails oder für kriminelle Aktivitäten genutzt. Es is daher in jedem Fall sinnvoll, wenn Sie die Server bei Verdacht mit einem oder mehreren Tools nach den Schädlingen durchsuchen lassen. Die bekanntesten Werkzeuge in diesem Bereich sind:

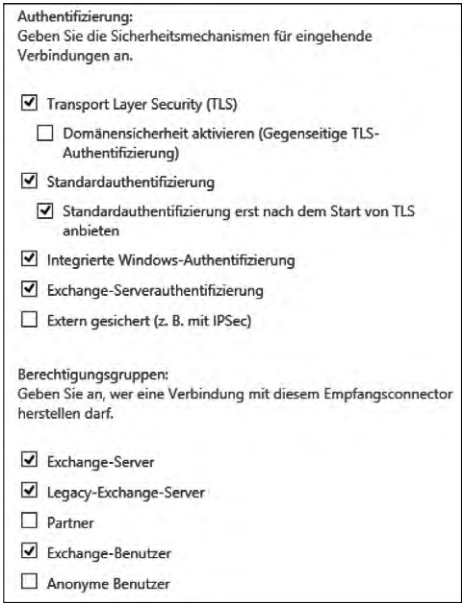
Bot-Bekämpfer	Rootkit-Bekämpfer
Malicious Software Removal Tool	Kaspersky TDSSKiller Rootkit Removal
Trend Micro RuBotted	avast! aswMBR Rootkit Scanner
Norton Power Eraser	Bitdefender Rootkit Remover
Avira	Malwarebtytes Anti-Rootkit
Kaspersky DE-Cleaner	McAfee Rootkit Remover
	Sophos Rootkit Removal Tool
	Oshi Unhooker
	Trend Micro RootkitBuster

1.1.3 Offenes Relay auf dem E-Mail-Server

Die Anzahl Ihrer Transaktionsprotokolle auf den Exchange-Servern wächst sehr schnell an, wenn Ihr Exchange-Server als offenes Relay im Internet steht. Dabei wird er von anderen Servern als Zwischenstation (Relay) zum Versenden von Spam oder Viren verwendet. Stellen Sie sicher, dass nur speziell eingetragene Server Ihren Exchange-Server als Relay verwenden dürfen, und am besten nur jene in Ihrem internen Netzwerk. Die Einstellungen dazu finden Sie in den Berechtigungen der Empfangs- und Sendeconnectoren, je nach der Exchange-Version, die Sie einsetzen. Spätestens dann, wenn Sie bemerken, dass Ihr Server auf schwarzen Listen der Spam-Versender erscheint, sollten Sie eine genaue Analyse von Exchange vornehmen und sicherstellen, dass kein Angreifer den Server dazu missbraucht, Spams oder Viren zu versenden.

In vielen Unternehmen gibt es Server, zum Beispiel ERP-, CRM- oder auch SharePoint-Server, die für ihre Funktionen einen E-Mail-Server auf SMTP-Basis ansprechen müssen, um E-Mails zu senden. Dies gilt auch für Multifunktionsgeräte oder Scanner. Aus Sicherheitsgründen blockiert Exchange E-Mails, die nicht von internen Anwendern kommen. Dabei ist es unerheblich, ob Exchange E-Mails intern zustellen oder über entsprechende Connectors nach außen versenden soll. Ist das Relaying für den Server deaktiviert, erhalten andere Server die Meldung: *550 5.7.1 Unable to relay*. In diesem Fall ist der Server sicher. Sie finden diese Einstellungen über *Nachrichtenfluss / Empfangsconnectors*.

Authentifizierung und Berechtigungsgruppen: Überprüfen Sie, ob die Sicherheitseinstellungen Ihrer Empfangs-Connectoren manipuliert wurden.



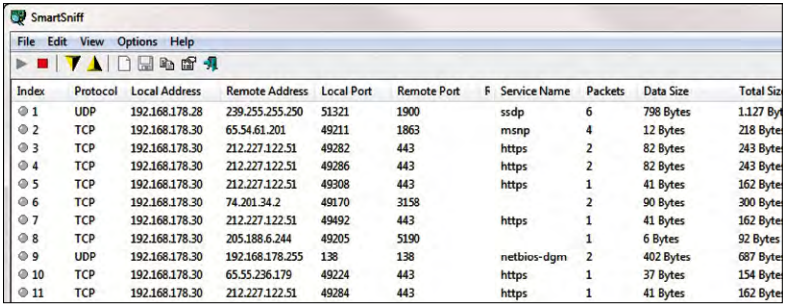
1.1.4 Verdächtigen Netzwerkverkehr finden

Angreifer auf Server äußern sich häufig auch durch verdächtigen Netzwerkverkehr. Hier müssen Sie sich ein wenig mit der Analyse von Netzwerken auskennen, um Angriffe zu finden. Mit dem kostenlosen **Microsoft Network Monitor** können Sie den Datenverkehr in Netzwerken verfolgen. Dabei muss es sich nicht immer um Microsoft-Netzwerke handeln (www.microsoft.com/download/en/details.aspx?id=4865). Das Tool steht im Microsoft Download-Center zur Verfügung. Informationen zu diesem Tool finden Sie auf den folgenden Seiten:

- **Blog zu Microsoft Network Monitor**
  (http://blogs.technet.com/b/netmon)
- **Network Monitor Open Source Parsers**
  (http://nmparsers.codeplex.com)
- **Network Monitor Experts**
  (http://nmexperts.codeplex.com)
- **TechNet-Forum**
  (http://social.technet.microsoft.com/Forums/en/netmon/threads)

Mit *New Capture / Start* beginnen Sie einen Scanvorgang. Auf den Seiten erhalten Sie auch Anleitungen, wie Sie Filter setzen und den Verkehr dadurch übersichtlicher überwachen können. Sie können den Scan-Vorgang auch abspeichern und

an Spezialisten senden, die die Daten besser auswerten können. Neben dem **Microsoft Network Monitor** können Sie auch das Tool **Wireshark** (www.wireshark.org) nutzen. Auch dieses ermöglicht eine Analyse des Netzwerkverkehrs. Um das Tool optimal nutzen zu können, müssen Sie noch Fehler! Hyperlink-Referenz ungültig. installieren, eine Erweiterung für Windows, die es Netzwerkprogrammen erlaubt, den Datenverkehr mitzuschneiden.



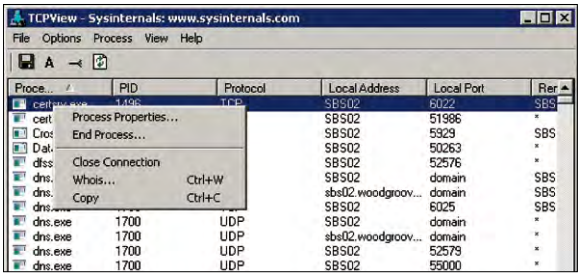
Index	Protocol	Local Address	Remote Address	Local Port	Remote Port	F	Service Name	Packets	Data Size	Total Siz
1	UDP	192.168.178.28	239.255.255.250	51321	1900		ssdp	6	798 Bytes	1.127 Byt
2	TCP	192.168.178.30	65.54.61.201	49211	1863		msnp	4	12 Bytes	218 Byte
3	TCP	192.168.178.30	212.227.122.51	49282	443		https	2	82 Bytes	243 Byte
4	TCP	192.168.178.30	212.227.122.51	49286	443		https	2	82 Bytes	243 Byte
5	TCP	192.168.178.30	212.227.122.51	49308	443		https	1	41 Bytes	162 Byte
6	TCP	192.168.178.30	74.201.34.2	49170	3158			2	90 Bytes	300 Byte
7	TCP	192.168.178.30	212.227.122.51	49492	443		https	1	41 Bytes	162 Byte
8	TCP	192.168.178.30	205.188.6.244	49205	5190			1	6 Bytes	92 Bytes
9	UDP	192.168.178.30	192.168.178.255	138	138		netbios-dgm	2	402 Bytes	687 Byte
10	TCP	192.168.178.30	65.55.236.179	49224	443		https	1	37 Bytes	154 Byte
11	TCP	192.168.178.30	212.227.122.51	49284	443		https	1	41 Bytes	162 Byte

SmartSniff: Bietet einen einfachen Mitschnitt des aktuellen Netzwerkverkehrs auf einem Computer.

Wenn Sie nur eine schnelle Übersicht über den aktuellen Datenverkehr sowie über die verschickten Pakete erhalten wollen, ohne einen Treiber installieren oder die Anwendung kompliziert einrichten zu müssen, ist **SmartSniff** (www.nirsoft.net) die richtige Wahl. Sie können das Tool ohne Installation direkt starten. Nach dem Start klicken Sie auf das grüne Dreieck, um den Sniffer-Vorgang zu starten.

1.1.5 Geöffnete Ports analysieren

Viele Schädlinge arbeiten mit eigenen Ports bei den Verbindungen zu Ihrem Heimatserver. Neben den Programmen für die Netzwerkanalyse sollten Sie daher auch die geöffneten Ports auf einem Server im Auge behalten und verdächtige Kommunikationsvorgänge überprüfen.



TCPView: Mit dem kostenlosen Tool lassen Sie sich Netzwerkverbindungen von Servern anzeigen.