Sichere Windows-Infrastrukturen

Das Handbuch für Administratoren

DAS VORWORT

Geleitwort des Fachgutachters

Sicherheit und Gesundheit sind in diesen Tagen besonders relevante Begriffe, denn wie schnell Viren ein System zum Stillstand bringen können, demonstriert gerade die Biologie. Aber auch ein IT-System kann schnell lahmgelegt werden, besonders dann, wenn die erste Infektion lange unerkannt bleibt und sich der Angriff im ganzen System ausbreiten kann. Und es gibt noch eine weitere Parallele: Auch IT-Umgebungen sind ohne passende Schutzmaßnahmen der Ausbreitung von Schadsoftware und Hacking-Angriffen schutzlos ausgeliefert.

Leider sind IT-Infrastrukturen so divers und komplex, dass auch die Software-Hersteller nur Empfehlungen für den produktiven Einsatz abgeben können. Wie die Systeme für den Anwendungsfall konfiguriert werden sollen, hängt von vielen Faktoren ab – es gibt schlicht keine perfekten Vorgaben, die ideal in jedem Szenario funktionieren und erzwungen werden können. Leider – oder zum Glück – gilt stattdessen: Es kommt auf Sie an, den Admin.

Kein Hersteller weiß, welche Systeme Sie über Jahre in Ihrer Infrastruktur aufgebaut und in Betrieb genommen haben. Daher finden Sie hier generische, aber praxisrelevante Ansätze, die Ihnen helfen, die Strukturen dieser gewachsenen Umgebungen zu verstehen. Dazu ist die Kenntnis der grundsätzlichen Konzepte unausweichlich.

Jeder Admin muss sich mit den Konfigurationsoptionen und Grenzen von sicherheitsrelevanten Einstellungen auseinandersetzen, um die für die jeweilige Umgebung optimale und damit »passendste« Entscheidung zu treffen. Gleichzeitig muss er die Angriffsvektoren, -methoden und -werkzeuge kennen, um überhaupt in der Lage zu sein, diese Entscheidung auch umzusetzen.

In diesem Buch werden Sie von *Tier-Levels*, *Systemhärtungen* und der *administrativen Trennung* lesen. All das sind sinnvolle und notwendige Schritte auf dem Weg zu einem sicheren System. Was beim ersten Blick ins Inhaltsverzeichnis wie eine große Baustelle mit unendlich vielen Gewerken aussieht, wird sich am Ende zu einem richtigen Gebäude zusammenfügen.

Die Beschreibungen und Anleitungen liefern Ihnen zahlreiche Anstöße, mit denen Sie kleine und größere Konfigurationen in Ihrer IT-Umgebung durchführen können und sich so gegen die klassischen Bedrohungen und Fehlkonfigurationen absichern. Security wird dabei zu einer Daueraufgabe – es gibt kein »Angekommen«, aber immerhin ein »Unterwegs« auf einer langen Security-Reise.

Die Frage, die sich Ihnen dabei wahrscheinlich stellt, lautet: »Geht es nicht auch ohne diesen ganzen Aufwand?« Die Realität zeigt leider, dass die Antwort »Nein« lauten muss: Die Liste der Firmen und Organisationen, die aufgrund lascher und nachlässiger Security-Einstellungen in eine schwierige Situation geraten sind, mit Datenver-

lust kämpfen mussten oder die Kontrolle über ihr Firmennetzwerk verloren haben, ist viel zu lang. Machen Sie es also besser!

Dazu bietet Ihnen das Buch die notwendige Basis: Sie finden einen Einstieg in den Bereich Angriffsvektoren und -Tools und viele Optionen zur Optimierung der eigenen Sicherheitslage. Gehen Sie es also an, beginnen Sie mit den ersten Optimierungen, und arbeiten Sie sich durch die verschiedenen Kapitel!

Daher bleibt mir nur noch, Ihnen viel Spaß beim Lesen und Umsetzen der Beispiele und Hinweise zu wünschen, die meine sehr geschätzten Kollegen aus der Praxis für Sie aufbereitet haben.

Raphael Rojas

Infrastrukturspezialist