LANline

9,– €

Juli 2016
20. Juni

ITP VERLAG

IT ■ Netze ■ Infrastruktur www.lanline.de

Datacenter Security und Hochverfügbarkeit

IT-Abwehrstrategie als Voraussetzung

Physische RZ-Sicherheit gemäß DIN EN 50600

Incident-Response-Management

Mit Marktübersicht USVs

Citrix Synergy in Las Vegas
Windows 10 aus der Cloud

Sonderschwerpunkt Monitoring
Blick auf Performance und Schwachstellen

Sonderdruck für mod IT Services
Mehr Pflicht als Kür

Schwachstellenscans selbst aufsetzen

Mehr Pflicht als Kür

Ein solides Patch-Management für alle Systeme ist zweifellos die Basis einer gepflegten IT-Infrastruktur. Dass dies nicht alle Lücken beseitigt, steht allerdings ebenfalls außer Frage. Schwachstellenscanner helfen, weitere Defizite zu erkennen. Über den Aufwand, ein professionelles und systematisches Schwachstellen-Management im Unternehmen zu etablieren, lässt sich trefflich diskutieren.

Auch das beste Patch-Management lässt Sicherheitslücken zurück. Manche Teile der IT-Infrastruktur entziehen sich beispielsweise der vollen Kontrolle der Administratoren, weil sie ein Dienstleister hostet oder managt. Bisweilen lassen sich auch die Softwarehersteller zu viel Zeit, um Updates auszuliefern. Hin und wieder sind die Patches auch fehlerhaft und flicken die vorhandenen Löcher nur unzureichend. Hinzu kommen noch die hochsensiblen und geschäftskritischen Systeme im Unternehmen, bei denen jeder Administrator zweimal überlegt, bevor er irgendetwas ändert – und sei es nur die Version einer installierten Software.

Vielfach eingesetzt in Penetrationstests: die Security-Linux-Distribution „Kali Linux“, unter der auch Schwachstellenscanner laufen können.

Lücken aufspüren

Mit Schwachstellenscans spürt man die vom Patch-Management zurückgelassenen Lücken zuverlässig auf. Dennoch nutzen viele IT-Abteilungen diese Werkzeuge nur unregelmäßig oder wenn die Governance-Vorgaben es zu bestimmten Audit-Terminen vorschreiben. Viele Unternehmen beauftragen Dienstleister mit dem Scannen der Infrastruktur – ein sinnvoller Weg, wenn das Know-how oder die Ressourcen im eigenen Hause fehlen. Dabei taucht immer wieder die Frage auf, ob man die Scanaufgaben nicht selbst übernehmen könnte.

Auch wenn bereits ein Tool für den Scan ausgewählt ist, sind einige Vorbereitungen zu treffen. Mit dem Blick auf die gesamte Infrastruktur muss der Verantwortliche zunächst klären, wer seitens der IT-Abteilung mit einzubeziehen ist und wie sich die Infrastruktur verteilt. Letzteres ist wichtig, weil es bei extern gehosteten Systemen notwendig sein kann, eine Einverständniserklärung des Dienstleisters einzuholen.

Eigentümer benachrichtigen

Informieren sollte man die Systemeigentümer in jedem Fall, um Missverständnisse zu vermeiden. Kompliziert wird es, wenn Applikationen auf Shared-Plattformen wie etwa bei Public-Cloud-Services laufen. In diesem Fall ist es nicht ohne Weiteres möglich, die Systeme zu scannen. Zum einen managen Provider ihre Systeme selbst – einer der dedizierten Vorteile von Cloud Computing – und lassen sich daher ungern hineinreden. Zum anderen liegen unter Umständen Daten und Applikationen anderer Kunden des Providers auf derselben Plattform. Dies macht einen Scan datenschutzrechtlich schwierig.

Genauso wichtig ist es, die operativen Administratoren und das für das Monitoring zuständige Team von Beginn an einzubeziehen. Denn ein Schwachstellenscan sieht für die verschiedenen Security- und Monitoring-Systeme unter Umständen wie ein Angriff aus. Es gilt, die Verantwortlichen für die Firewall, das Intrusion-Prevention-System (IPS), das Intrusion-Detection-System (IDS) oder das Security-Information- and Event-Management (SIEM) unbedingt vorher zu informieren. Denn spätestens wenn der Scan zahlreiche Logs und False Positives (Fehlalarme) produziert, sind die Administratoren im Stress. Vorherige Absprachen und entsprechend

zusammengestellte Projektteams vermeiden solche Missverständnisse.

Innerhalb eines Teams von verantwortlichen Administratoren lässt sich auch der Termin für den Schwachstellenscan besser bestimmen. Denn dies ist keineswegs trivial: Zum einen kann der Scan wie beschrieben die Systeme beeinträchtigen oder aber eine schmalbandige LAN/WAN-Verbindung recht gut auslasten, sodass eher ein Termin außerhalb der Hauptgeschäftszeiten infrage kommt. Zum anderen lassen sich eben genau während der Kernarbeitszeiten die meisten Client-Systeme über das Netzwerk erreichen. So ist es sinnvoll, Clients und unkritische Server tagsüber zu scannen und die Arbeit an den hochkritischen Systemen außerhalb der Geschäftszeiten oder an einem definierten Wartungstag durchzuführen. Mit der Zeit bekommen die Verantwortlichen ein Gefühl dafür, welchen Einfluss der Scanner auf die verschiedenen Systeme hat, und können bei Bedarf das Timing der Aktivitäten nochmals überdenken.

Die meisten Scanner wie zum Beispiel der Nessus Vulnerability Scanner von Tenable liefern bereits in der vom Hersteller ausgelieferten Grundkonfiguration brauchbare Ergebnisse. Fehlen dem Tool jedoch individuelle Parameter der Umgebung, besteht die Gefahr, dass es wichtige Schwachstellen übersieht. Vor dem ersten Einsatz sollte der Schwachstellenscanner daher einmal durchkonfiguriert und den individuellen Ausprägungen der IT-Landschaft angepasst werden. Manche Softwarehersteller lassen Peripheriegeräte wie etwa Drucker per Werkseinstellung nicht mitscannen, da diese häufig instabil auf einen Schwachstellenscan reagieren. Doch dass gerade Drucker vom Scan nicht ausgenommen sein sollten, ist von großer Bedeutung: Schließlich verarbeiten sie oft sensible Daten.

Die meisten Scanner bieten Zugang zu nützlichen Plug-ins, die sich aktivieren lassen. Doch ist dazu Expertenwissen gefragt, die Option „nur sichere Scanner-Plug-ins verwenden“ ist aus gutem Grund meist voreingestellt. Denn bereits das Aufspüren einer Sicherheitslücke kann zu einem „Denial of Service“-artigen Szenario führen – erst recht, wenn die Plug-ins nicht genügend abgesichert sind. Allerdings liefern entsprechende Plug-ins häufig interessante Zusatzinformationen, da sie oft nur eine spezielle Applikation oder Schwachstelle überaus gründlich prüfen – ob das das Risiko eines instabilen Netzwerkes wert ist, müssen die Verantwortlichen im Einzelfall entscheiden.

Das Scannen von Netzwerken und offenen Ports ist eine grundlegende Maßnahme der IT-Sicherheit. Ein häufig genutzter Portscanner ist Nmap.

Gewöhnliche Schwachstellenscans betrachten das Netzwerk von außen, so wie ein Hacker es sehen würde. Das sogenannte Credentialed Scanning geht darüber hinaus: Der Scanner erhält dabei Login-Daten, mit denen er sich auf dem Zielsystem einloggt. Dies hat verschiedene Vorteile: Der Scan-Vorgang verursacht so insgesamt weniger Traffic und, da er ja im Netzwerk autorisiert ist, keinen, der als Angriff eingestuft wird. Zudem kann ein Credentialed Scan – eben weil er praktisch im Inneren stattfindet – mehr Informationen liefern und auch Client-Applikationen oder Server-Dienste hinter Firewalls scannen, die vom Scanner nicht direkt erreichbar sind.

Die Auswertung ist wahrscheinlich der schwierigste Teil, wenn den Schwachstellenscan nicht ein Dienstleister, sondern die eigene IT-Administration durchführt. Die Informationen sind zahlreich sowie in die Rubriken kritisch und unkritisch zu kategorisieren. Die Software liefert bereits gute Vorarbeit, doch ist es nicht einfach zu unterscheiden, ob nicht ein Zusammenspiel unkritischer Ereignisse zu einem kritischen Event geführt hat. Dann ist es hilfreich, zumindest am Anfang einen Experten zu Rate zu ziehen. Der Schwachstellenscan ist nur dann sinnvoll, wenn sich daraus konkrete Schritte zur Absicherung der IT-Infrastruktur ableiten lassen.

Die IT-Umgebung regelmäßig scannen

Der wirkliche Nutzen des Schwachstellenscans entfaltet sich, wenn er regelmäßig durchgeführt wird. Die IT-Administratoren erhalten dann schnell ein Gefühl dafür, welche Systeme durch den Scan in ihrer Arbeit beeinflusst werden, und können den nächsten Time-Slot besser planen. Die IT-Experten, die die Daten auswerten, haben bald vergleichbare Informationen, die über die Momentaufnahme eines einmaligen Scans hinausgehen. Und das IT-Management kann auf diese Weise verfolgen, ob identifizierte Schwachstellen nun gepatcht sind.

Sebastian Brabetz/jos

Sebastian Brabetz ist IT Security Engineer bei Mod IT Services, www.it-mod.de.