Schichtenmodell für mehr Sicherheit

von Rainer Richter, avecto

So unverzichtbar sie auch sind: Firewall und Antivirus-Software allein reichen für den Endgeräte-Schutz nicht mehr aus. Angesichts wachsender Cyber-Gefahren und immer raffinierterer Angriffsmethoden benötigen Windows-Clients heute ein proaktives Zusammenspiel verschiedenartiger Security-Mechanismen.

Von Microsoft Internet Explorer über Adobe Flash und Google Chrome bis zu Mozilla Thunderbird: das Bundesamt für Sicherheit in der Informationstechnik (BSI) registrierte bei elf weit verbreiteten Softwareprodukten zwischen Januar und September 2015 nicht weniger als 847 kritische Schwachstellen.

Grundsätzlich empfiehlt das BSI, alle von Herstellerseite aus angebotenen Security-Patches stets so schnell wie möglich einzuspielen. Doch keine noch so große Update-Disziplin kann hundertprozentigen Schutz vor böswillig eingeschleuster Schadsoftware garantieren. Ein Patch schließt immer nur bereits be- bzw. erkannte Sicherheitslücken und verkürzt dadurch die Zeitspanne, innerhalb derer ein Hacker diese Lücke für einen Angriff ausnutzen kann. Gegen sogenannten Zero-Day-Exploits jedoch bleiben Client-Geräte trotz Antivirus-Aktualisierung ungeschützt. Solche Cyber-Angriffe zielen auf offene Schwachstellen, für die es noch keine Patches gibt. Besonders bedrohlich wird die Situation, wenn bereits Informationen über Zero-Day-Schwachstellen in der Hacker-Szene kursieren. Oftmals werden dafür sogar maßgeschneiderte Angriffswerkzeuge auf dem Schwarzmarkt im Internet gehandelt.

Verwundbar sind Client-Geräte nicht zuletzt durch den Siegeszug der Browsernutzung: Ein tückisches Angriffsmittel sind hierbei die sogenannten Drive-by-Exploits: Sie nutzen Schwachstellen im Webbrowser oder einem Browser-Plug-in, um heimlich ein Schadprogramm zu installieren. Zur Infektion genügt lediglich der Aufruf einer entsprechend präparierten Webseite.
Drive-by-Gefahr besteht keineswegs nur bei dubiosen Internetangeboten, sondern ebenso auf seriösen Seiten. Laut BSI-Bericht enthalten deutschlandweit ein bis zwei Prozent aller Webseiten Drive-by-Exploits oder verweisen auf andere kompromittierte Seiten.

Insgesamt ist in den letzten Jahren eine Professionalisierung der kriminellen Szene zu beobachten, was unter anderem an den zunehmend ausgefeilten Social-Engineering-Angriffen und der Häufigkeit gezielter Advanced Persistent Threats deutlich wird.

Admin-Rechte: die unterschätzte Gefahr

Reaktive Sicherheitsvorkehrungen wie Antivirus- und Firewall-Lösungen sollten durch eine zusätzliche Schicht aus proaktiven Schutz- und Abwehrkomponenten ergänzt werden. Empfehlenswert ist eine Layer-basierte Sicherheitsarchitektur deshalb, weil vorhandene Lösungsbausteine wie etwa die Applikationskontrolle effektiver werden, ohne dass das Security-Management als Ganzes dadurch komplizierter würde.

Ein ebenso einfacher wie wirkungsvoller Ansatz dafür besteht beispielsweise in einer möglichst restriktiven Vergabe von Administratorrechten für Endgeräte-Nutzer. Dahinter steht die einfache Erkenntnis, dass unbemerkt infiltrierte Malware auf betroffenen Systemen umso weniger Schaden anrichten kann, je weniger Privilegien dem jeweiligen Nutzer-Account zugeordnet sind. Auch die Ausbreitung eingedrungener Schadsoftware auf andere Rechner im Unternehmensnetzwerk wird somit eingedämmt.

Sobald allen Mitarbeitern – mit Ausnahme der IT-Administratoren – ausschließlich Standardnutzerrechte zugebilligt werden, lassen sich Risiken bei 96 Prozent aller kritischen Microsoft-Schwachstellen signifikant verringern. Denn eine Schadsoftware kann dann weder Systemänderungen noch nicht-autorisierte Programminstallationen vornehmen. De facto hätten 2013 sämtliche Angriffsversuche über Sicherheitslücken im Microsoft Internet Explorer allein durch Rückstufung der betroffenen Systeme auf Standardprivilegien gestoppt werden können.

Berechtigungsmanagement in der Praxis

Doch wie sieht die derzeitige Praxis in den meisten Unternehmen aus? Mehr als 30 Prozent von ihnen haben keinerlei Richtlinien zur Vergabe von Admin-Privilegien festgeschrieben. In 72 Prozent aller Fälle besitzen zeitweilig beschäftigte Mitarbeiter Administratorenrechte. Und dies, obwohl das Rechtemanagement seit der Einführung von User Account Control (UAC) in den aktuellen Windows-Versionen um ein Vielfaches einfacher geworden ist.

Selbstverständlich benötigen Fachkräfte in der IT-Abteilung – neben Administratoren zum Beispiel auch Anwendungsentwickler – weiterhin die Möglichkeit, tiefer in das System einzugreifen. Aber auch bei anderen User-Gruppen darf die tägliche Nutzung nicht durch undifferenzierte Rechterestriktionen erschwert werden.

In der Praxis bewähren sich hierbei am besten rollenbasierte Privilegien-Management-Lösungen, die auf betriebssystemeigenen Tools wie UAC aufsetzen und mehr Flexibilität bei der Rechtevergabe ermöglichen. Wichtig ist zudem eine enge Integration in die Anwendungsverwaltung, sodass bestimmte Zugriffsrechte aus dem Nutzungskontext heraus direkt von einer Applikation erteilt werden können. Der betreffende User erhält situationsbezogen alle notwendigen Privilegien, wird aber nicht pauschal auf ein zu hohes Rechte-Level angehoben.

Der Nutzungskomfort ist beim Rechtemanagement ein nicht zu unterschätzender Aspekt, bei dem es nicht nur um Help-Desk-Entlastung geht, sondern vor allem um die Akzeptanz der IT-Sicherheitsstrategie im Unternehmen. Und deren Erfolg ist auf eine breite Unterstützung der gesamten Belegschaft angewiesen.

Anwendungen effektiv kontrollieren

Bestandteil der Endgeräte-Sicherung im Windows-Betriebssystem ist ein signaturbasierter Erkennungsansatz, um potenziell schädliche Software aus nicht vertrauenswürdiger Quelle zu erkennen. Allerdings schafft es heutzutage mehr als die Hälfte aller Schadprogramme, diesen Anwendungsfilter zu durchdringen.

Ein weitaus effektiveres Verfahren bietet eine aktive Applikationskontrolle: Zugelassen werden dabei nur solche Anwendungen, die vom IT-Team geprüft und ausdrücklich für den Einsatz im Unternehmen bestätigt worden sind. Diese traditionell schwierige Herangehensweise endet schnell in einem erhöhten Wartungsaufwand für die Erstellung und Pflege einer solchen Whitelist.

Hier hilft ein intelligenter Ansatz weiter, bei dem die vertrauenswürdigen Applikationen auf der Grundlage von bekannten Systemverzeichnissen und standardisierten Referenzsystemen des Unternehmens freigegeben werden, die den administrativen Aufwand auf ein Minimum zu reduzieren. Dies verhindert die Installation und Ausführung von Malware und dem unkontrollierten Softwaredownload argloser Mitarbeiter ist damit automatisch ein Riegel vorgeschoben.

Sandkastenspiele? Aber sicher!

Indes verbergen sich weitere Gefahrenquellen in unterschiedlichsten Dokumenten, die aus dem modernen Arbeitsalltag nicht mehr wegzudenken sind, etwa PDF- und Office-Dateien. Dazu folgendes Beispiel: Ein Mitarbeiter lädt ein infiziertes Dokument aus dem Internet herunter, oder die Webseite ist mit einem Drive-by-Exploit infiltriert.

Der Angriff bleibt unentdeckt; die Datei wird von einem durch die Applikationskontrolle bestätigten Programm wie dem Internet Explorer, einer Office-Anwendung oder dem Adobe Acrobat Reader geöffnet. Weder die Antivirussoftware noch die Anwendungskontrolle schlägt Alarm, sodass der Schadcode nahezu ungehindert auf Daten und Programme des befallenen Endgeräts zugreifen kann.

Downloads aus dem Internet gänzlich zu verbieten, ist im Online-Zeitalter sicherlich keine vernünftige Option. Ratsam ist stattdessen das sogenannte Sandboxing, bei dem alle Inhalte aus unbekannter Quelle in einem isolierten Bereich – eben der Sandbox – gespeichert werden. Getrennt von Daten und Programmen können sie somit keinerlei Schaden auf dem Endgerät verursachen.

Ein großer Vorteil des Sandkastenprinzips besteht darin, dass es bei intelligenter Umsetzung so gut wie keine Nutzungseinschränkungen für die Anwender mit sich bringt. Intelligent heißt in diesem Kontext, dass eine entsprechende Lösung zum Beispiel sämtliche Dokumente klassifiziert, nachvollzieht und alle Dateien aus dem Internet ausschließlich in der Sandbox ablegt. Dort können sie beliebig geöffnet, geändert und ausgedruckt werden – ohne die Sicherheit des Endgerätes im Geringsten zu bedrohen.