Mit SecuLution ausgetretene Pfade in der IT-Sicherheit verlassen

Positiv- statt Negativliste

Die itsa, Europas größte Messe für IT-Sicherheit, hat es wieder einmal gezeigt: Das Thema Security brennt deutschen Gesundheitseinrichtungen unter den Nägeln. Gefragt sind innovative, aber einfach zu administrierende Lösungen. Besonders hinterfragt wird die Wirksamkeit der angebotenen Lösungen, da Angriffe sowohl in Deutschland und Großbritannien als auch weltweit in den letzten zwei jahren gezeigt haben, dass die üblichen Mechanismen von Virenscannern und Firewalls keinen ausreichenden Schutz mehr bieten können.

Nie wieder Viren, Trojaner oder Ransomware. Das verspricht die IT-Sicherheitsfirma SecuLution. Die gleichnamige Application Whitelisting Lösung setzt dabei auf eine White- statt eine Blacklist. Der Ansatz ist dabei denkbar einfach. Während Virenscanner immer kompliziertere Mechanismen etablieren müssen, um die neuesten Bedrohungen auch erkennen zu können, reicht es beim Application Whitelisting nur das ausführen zu lassen, was auch vertrauenswürdig ist. Alles andere wird blockiert.

Nie wieder Schadsoftware

„In den allermeisten Fällen liegt der Befall von IT-Systemen im Krankenhaus mit Ransomware im Versagen der Schutzvorkehrungen begründet“, erläutert SecuLution-Geschäftsführer Torsten Valentin. „Wobei die Virenscanner an sich gar nicht versagen, denn ihr Wirkprinzip ist, den Angriff von bekannter Schadsoftware zu verhindern. Und genau darin liegt die größte Schwachstelle: Die Täter hinter Viren- und Ransomware-Attacken erzeugen mehrfach täglich neue Versionen der Schadsoftware. Die Hersteller von Virenscannern haben also keine realistische Chance, vor der Erstverbreitung jeder Version die Schutzmechanismen anzupassen.“ Die Folge: Jede neue Version findet erst einmal unzählige Opfer.

SecuLution Application Whitelisting bietet Sicherheit für alle Endpoints, Desktops wie Server und schützt so gleichzeitig das Netzwerk vor ungebetenen Eindringlingen. Eine zentrale Whitelist im Netzwerk sorgt dafür, dass komplizierte Sicherheitskonstrukte überflüssig werden. Ressourcenfressende Echtzeitscans gehören der Vergangenheit an, versehentlich verdächtigte Software, die in Quarantäne genommen wurde und erst umständlich wieder freigegebenen werden muss, ebenso. „Unsere Anwender sind optimal geschützt, gerade weil die Frage, ob eine Software vertrauenswürdig ist und ausgeführt werden soll, künftig durch geschultes Fachpersonal getroffen wird. Einfach und sicher“, stellt Valentin heraus.

„Application Whitelisting ist der einzig effektive Schutz vor unbekannter Software“

So einfach der Schutz mit SecuLution funktioniert, so schnell ist die Lösung auch im Netzwerk installiert und eingerichtet. Der Clou des SecuLution-Systems ist die innovativ einfache Art, wie selbst in großen Netzwerken die erwünschte Software gelernt und identifiziert wird. Sie brauchen keine riesige IT Abteilung für die Verwaltung und Konfiguration, da die meisten Abläufe automatisiert sind. Im Gegensatz zu anderen Whitelisting Lösungen arbeitet SecuLution ausschließlich mit den Hashes – den elektronischen Fingerabdrücken – der erlaubten Software. Beim starten jeglicher Software wird der Hash dieser Software gebildet und gegen die Whitelist geprüft; ist der Hash nicht als derjenige einer erwünschten und vertrauenswürdigen Software auf der Whitelist erfasst, kann die Software nicht ausgeführt werden. Besonders einfach ist dabei die erste Erfassung der erlaubten Software. „Über Musterrechner und ein spezielles Lernverfahren erfassen wir innerhalb kurzer Zeit sämtliche Software und durch einen Abgleich mit unserer Cloud basierten Datenbank können die gelernten Hashes schnell in vertrauenswürdig oder schadhaft unterteilt werden. Auch in großen Netzwerken mit unzähliger Spezialsoftware und verschiedenen Versionsständen, wie es zum Beispiel oft in Krankenhäusern der Fall ist. Dank der vollautomatischen Erfassung der Hashes von Programmupdates wird der Administrationsaufwand gering gehalten, die Sicherheit aber maximal erhöht. So schafft unsere Lösung den Administratoren Ressourcen für das Tagesgeschäft“, erläutert Valentin die Implementierung.

SecuLution bezieht nicht nur den ausführbaren Code einer Software mit in den Whitelisting-Mechanismus ein, vielmehr können auch Java Code, DLL-Dateien oder USB-Geräte als vertrauenswürdig auf der Whitelist geführt und verwaltet werden. Da SecuLution offlinefähig ist, werden sogar Geräte, die nicht ständig mit dem Netzwerk und der Positivliste verbunden sind, durch die Lösung geschützt.

„Application Whitelisting ist der einzig effektive Schutz vor unbekannter Software. Die Erstellung und Pflege einer Whitelist ist weder zeitintensiv noch aufwändig. Im Gegenteil, vieles kann problemlos automatisiert werden, so dass Administratoren sich nicht einen Großteil ihrer Zeit um ihre Sicherheitslösung kümmern müssen“, verdeutlicht Torsten Valentin die Einfachheit der Lösung.

www.seculution.de