Application Whitelisting als wirksame Endpoint Protection

Application Whitelisting ist weitaus sicherer, als jede andere Antivirus Technologie, hat aber den Ruf, einen höheren Administrationsaufwand zu erzeugen. Wir haben fünf Krankenhäuser befragt, die SecuLution Application Whitelisting einsetzen.

Cyberangriffe auf Gesundheitseinrichtungen – auch in Deutschland – haben in den letzten Jahren zugenommen. Ein wirksamer Schutz ist die Absicherung der Endpunkte, also der Computer, Server oder Workstations, mittels Application Whitelisting. Das verhindert das Ausführen von ungewollter Software, wie Viren, Trojaner oder Spiele.

Application Whitelisting ist ein technischer Ansatz, bei dem ein elektronischer Fingerabdruck jeglicher Software auf einer Freigabeliste vorhanden sein muss, damit die Software ausgeführt werden kann. Application Whitelisting stellt damit das Gegenteil des Virenscanners dar: Der Virenscanner erlaubt alles und verbietet als "schadhaft" bekannte Software. Application Whitelisting verbietet alles und erlaubt als "gut" bekannte Software. Die technische Herausforderung bei Virenscannern ist, dass auf der Blacklist (der Liste der verbotenen, "bösen" Software) jegliche Schadsoftware vorhanden sein muss. Kennt die Blacklist eine Schadsoftware nicht, wird die Software erlaubt und kann das Computernetzwerk infizieren. Die technische Herausforderung bei Application Whitelisting ist, dass auf der Whitelist (Liste der erlaubten Software) jegliche beruflich benötigte Software vorhanden sein muss. Kennt die Whitelist eine Software nicht, wird die Software verboten. Daher ist beim Einsatz von Application Whitelisting keine Infektion mit bekannter oder unbekannter Schadsoftware möglich.

Der deutsche Hersteller SecuLution GmbH hat auf der it-sa seine Cloud basierte Whitelist vorgestellt, mit der SecuLution Systeme automatisch live erlernen können. So wird die Freigabe von vertrauenswürdiger Standard-Software auf der Whitelist des Anwenders automatisiert aus der Cloud Datenbank des Herstellers übernommen. Anwender müssen nur noch etwaige Individualsoftware einpflegen.

Im Folgenden berichten Anwender des Application Whitelisting von SecuLution über ihre Erfahrungen mit der Lösung. Etwaige Wiederholungen in den Aussagen wurden gekürzt.

SecuLution GmbH
Alter Hellweg 6
59457 Werl
www.seculution.de
mailto:info@seculution.com

Katholisches Klinikum Lünen/Werne

Betten: ca. 600
IT-Systeme: 600
SecuLution Benutzer seit: 2006

Christian Hübener (operativer IT-Leiter): "Wir hatten vor dem Einsatz von SecuLution als Application Whitelisting Lösung einen Virenscanner. Unsere Sorge war, dass man den Antivirus nicht immer auf den aktuellen Stand hat und dadurch Opfer einer Bedrohung wird. Beispiel: Person A bringt einen Stick mit und darauf ist eine Schadsoftware. Derartige Probleme sind zuverlässig vom Tisch. [...] Wir setzen SecuLution Application Whitelisting daher inzwischen in allen Bereichen der Konzernstruktur ein."

St. Joseph-Stift Dresden

Betten: ca. 600
IT-Systeme: 550
SecuLution Benutzer seit: 2007

Rene Schumann (Systemadministrator): "Wir hatten mit SecuLution noch nie einen erfolgreichen Angriff mit Schadsoftware. Der technische Ansatz, nur die Ausführung von als gut bekannter Software möglich zu machen, gibt uns ein gutes und beruhigendes Gefühl, das vorher nicht da war. [...] Die Administrationsoberfläche von SecuLution ist unser sicherheitstechnischer zentraler Dreh- und Angelpunkt."

Marienkrankenhaus Schwerte GmbH

Betten: ca. 500
IT-Systeme: 450
SecuLution Benutzer seit: 2016

Marco van de Straat (stellvertretender IT-Leiter): "Ein Qualitätsmerkmal einer Software ist meiner Meinung nach, wenn man als Admin im Alltag möglichst wenig damit zu tun hat. Seit dem Update auf SecuLution 2.0, besonders durch die automatische Abfrage der TLDB [Anm: Cloud-basierte zentrale Whitelist als Serviceleistung von SecuLution], ist der Umgang auch viel einfacher geworden. [...] SecuLution hat auf jeden Fall einen großen Mehrwert für uns gebracht. Wir haben im Alltag relativ wenig mit der Administration von SecuLution zu tun!"

Rheinland Klinikum Neuss GmbH

Betten: ca. 700
IT-Systeme: 500
SecuLution Benutzer seit: 2016

Christoph Fischer (EDV Administrator): "Vor meiner Zeit [Anm.: 2016] hatten wir ein massives Problem! Unser Virenscanner hatte einen Angriff nicht erkannt. Unsere gesamte IT Struktur war mit Schadsoftware befallen. Es war den Medien zu entnehmen. Wir brauchten eine zuverlässige Lösung, damit derartiges nicht noch einmal passieren kann. [...] SecuLution Application Whitelisting erfüllt unsere Erwartungen voll."

St. Elisabeth - Hospital GmbH Beckum

Betten: ca. 220
IT-Systeme: 270
SecuLution Benutzer seit: 2005

Volker Kliewe (EDV Administrator): "Vor der Entscheidung für SecuLution als Application Whitelisting Lösung hatten wir trotz unseres aktuellen Virenscanners einen Befall mit Schadsoftware. Seit wir SecuLution Application Whitelisting einsetzen, haben wir überhaupt keine Probleme damit mehr. [...] Das permanente Kontrollieren der Arbeitsplätze, ob alle Updates der Virenscanner erfolgreich installiert waren, hat viel Zeit gefressen. [...] Mit SecuLution haben wir nur einen geringen Aufwand, weil die Umsetzung von Aktionen in Echtzeit passiert und die Reaktion des Programms absolut vorhersehbar ist."