Manche Administratoren machen es sich sehr einfach. Mit Whitelisting.

Jedes Jahr verursachen kriminelle Hacker-Banden mit Computer-Schädlingen wie Ransomware erhebliche Schäden. Ganze Unternehmen werden lahmgelegt und erpresst. Man schätzt, dass so allein in Deutschland letztes Jahr ein rein finanzieller Verlust von rund 50 Milliarden Euro entstanden ist. Doch wie können sich Unternehmen und Institutionen wie zum Beispiel Kliniken und Krankenhäuser wirksam vor solchen Cyber-Attacken schützen? Hier ein kurzer Überblick.

Was passiert bei einem Netzwerk-Angriff?

Es kann jeden treffen. Plötzlich funktioniert nichts mehr. Server und ganze Netzwerke spielen verrückt oder man verliert jeglichen Zugriff auf seine Daten. Schuld sind oft kriminelle Angriffe von professionell organisierten Banden. Jeden Tag starten rund 25.000 neue Schädlinge in den Wettlauf mit Anti-Virus-Programmen. Dabei legt die zunehmende Anzahl an Schadsoftware alle betroffenen Unternehmen bis zur Handlungsunfähigkeit lahm.

Was nützen Anti-Viren-Programme?

Die meisten Administratoren versuchen bislang, Netzwerk durch eine – oftmals teure – Anti-Viren-Software vor solchen Attacken zu schützen. Das Problem dabei ist, dass das Prinzip von Anti-Virus-Software aus den 80er Jahren stammt. Grundsätzlich schützt Virenscanner nur vor Schadsoftware die bereits bekannt ist oder die auffällig erscheint. Denn die Virenscanner schauen sich jedes Programm an und entscheiden dann, ob es eine bekannte Gefahr darstellen könnte. Das bedeutet, dass Programme, die dem Virenscanner noch nicht als gefährlich bekannt sind, ungehindert ausgeführt werden können. Das ist in etwa so, als wenn ein Türsteher jeden in mein Haus lässt, den er nicht kennt und nur den wegschickt, der als Unerwünscht bekannt ist. Neu entwickelte oder bis

zur Unkenntlichkeit modifizierte Schadsoftware kann sich weiterhin Zugang zu Netzwerken und Servern verschaffen und trotz Anti-Virus-Software erheblichen Schaden verursachen. Dass Virenscanner trotz immer neuen Begriffen wie z.B. Heuristik, Sandboxing, verhaltensbasierter Analyse usw. keinen zuverlässigen Schutz bieten, haben die Vorfälle in 2016 hinreichend gezeigt.

Die Folge: Die Zahl der erfolgreichen Angriffe gegen Netzwerke, um zum Beispiel Geld für gekidnappte Daten zu verlangen, hat seit dem letzten Jahr enorm zugenommen. Experten gehen sogar von einer Steigerung um mindestens 25 % aus. Davon betroffen sind auch viele Krankenhäuser. Das ist besonders fatal, da es im Gesundheitswesen um Millionen von sensiblen Patienten-Daten geht.

Die Bundesregierung hat hierzu 2015 das IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) verabschiedet. Es verpflichtet bestimmte Unternehmen zu einer Meldung von Angriffen an das BSI (Bundesamt für Sicherheit in der Informationstechnik) und zur Einhaltung der Sicherheitsstandards, die vom BSI erarbeitet wurden. Darüber hinaus fordert das BSI Betriebe dazu auf, ineffiziente Maßnahmen durch effizientere Security-Maßnahmen zu ersetzen. Dazu zählen zum Beispiel Whitelist-Lösungen.

Whitelisting – besser als ein Virenscanner?

Das Whitelisting-Prinzip ist so simpel wie effektiv: Während ein Virenscanner definiert, was verboten sein soll (Blacklist) und nur blockiert, was er kennt, also somit alles Unbekannte erlaubt, funktioniert eine moderne Whitelist-Lösung genau anders herum: Es wird definiert, was zur Arbeit benötigt wird (Whitelist). Alles, was nicht explizit als „erlaubt" eingestuft wurde, kann erst gar nicht gestartet werden. Damit wird sämtliche Schadsoftware automatisch als „unbekannt" eingestuft, kann nicht ausgeführt werden und daher auch keinen Schaden anrichten. Die SecuLution-Lösung schützt demnach nicht nur vor bereits bekannten, sondern auch vor den neuesten noch unbekannten Viren und anderen Schädlingen. Sie ist quasi der Türsteher, der nur Ihre Mitarbeiter in ihr Unternehmen lässt.

Was taugt Whitelisting wirklich?

Eine gute Whitelist-Lösung leistet dabei sogar mehr als ein reines Antivirus-Produkt. Während Virenscanner vor Schadsoftware schützen sollen, liefert SecuLution darüber hinaus eine moderne Endpoint-Security-Lösung und feingliedrige Rechteverwaltung. Denn was nicht für die tägliche Arbeit gebraucht wird und nicht ausdrücklich genehmigt ist, kann auch nicht von einem Mitarbeiter auf dem betrieblichen Rechner gestartet werden. Welchen genauen Funktionsumfang die Software bietet und wie es im Alltag eines Administrators funktioniert, lässt sich zum Beispiel in einer kostenlosen Onlinepräsentation des Herstellers erfahren.

Wie arbeitet SecuLution?

SecuLution arbeitet nach dem „Whitelisting"-Prinzip und schützt dadurch wirksam und verlässlich vor Schadsoftware. Während ein Virenscanner definiert, was verboten sein soll (Blacklist) und nur blockiert, was er kennt, also somit alles Unbekannte erlaubt, funktioniert SecuLution genau anders herum: Es wird definiert, was zur Arbeit benötigt wird (Whitelist). Alles, was nicht explizit als „erlaubt" eingestuft wurde, kann erst gar nicht gestartet werden. Damit wird sämtliche Schadsoftware automatisch als „unbekannt" eingestuft, kann nicht funktionieren und daher auch keinen Schaden anrichten. SecuLution ist damit sogar mehr als ein reines Antivirus-Produkt. Es ist eine moderne Endpoint Security-Lösung und feingliedrige Rechteverwaltung, die sehr viel mehr leistet als nur den Schutz des Computers vor Schadsoftware.

Können die gesetzlichen Vorgaben mit einer Whitelist eingehalten werden?

Auch die Erfahrungen aus der Praxis sprechen für Whitelistung: Seit die erste große Ransomwarewelle Ende letzten Jahres und Anfang diesen Jahres die Krankenhäuser erfasst und zum Teil enorm geschädigt hat, vermeldeten Kliniken, die bereits ein Whitelist-System von SecuLution einsetzen, keine Ausfälle. Hier hat die Absicherung durch SecuLution nachweislich geholfen, die erhöhte Anzahl von gezielten Angriffen abzuwehren. Dementsprechend registrieren die Experten von SecuLution eine gestiegene Nachfrage nach mehr Sicherheit:

„Dieses Jahr haben wir im Gesundheitswesen – größtenteils in Krankenhäusern – aufgrund der Bedrohungslage einen erhöhten Bedarf an unserer Sicherheitslösung feststellen können. Gleichzeitig wuchs auch das Interesse an modernen Sicherheitslösungen für große Firmennetzwerke, wie SecuLution sie mit dem Whitelsting-Prinzip bietet, erheblich."

Wie aufwendig ist Whitelisting für Administratoren?

Leider herrscht noch immer Unsicherheit. Viele Administratoren scheuen derzeit die Umstellung auf das Whitelist-Verfahren. Hauptgrund ist der befürchtete Aufwand: Die Whitelist muss einmalig erstellt und dann gepflegt werden, wenn Updates oder neue Software installiert werden müssen. Dabei bietet SecuLution hier eine einfache Lösung: Ein frisch installiertes System dient als Basis für die initiale Whitelist und wird dann in einem automatischen Lernprozess um

Abweichungen ergänzt. Das heißt während die Nutzer ganz normal weiterarbeiten lernt SecuLution im Hintergrund noch unbekannte Programme und Rechnerkonfigurationen. Diese neu gelernten Regeln kann der Administrator, nach beenden des Lernmodus mit nur einem Klick auf Vertrauenswürdigkeit prüfen lassen. Jetzt müssen lediglich die als nicht vertrauenswürdig eingestuften Programme wieder aus dem Regelsatz entfernt werden und die Whitelist ist fertig. Patches und Updates können ebenfalls über voll automatisierte Aufgaben aus festgelegten Verzeichnissen komfortabel dem Regelsatz hinzugefügt werden. Sie befinden sich somit für alle Nutzer bereits vor der Installation auf der Positivliste. Dieser Prozess bedeutet keinen nennenswerten Zeitaufwand für den Administrator. Das können die Anwender nur bestätigen. So erklärt Dirk Andrae vom Krankenhaus St. Joseph-Stift in Dresden:

„Ich war besorgt, dass die Erstellung und Pflege einer Whitelist der vertrauenswürdigen Anwendungen und Geräte viel, viel Arbeit wäre. Aber das war überhaupt kein Problem. Alles war in wenigen Arbeitsstunden erledigt."

Fazit: Mit einem Whitelist-Schutz wie dem von SecuLution können Systeme nicht mehr mit Schadsoftware infiziert werden. Dadurch entfallen aufwändige Neuinstallationen von befallenen Computern. Die Benutzer können während ihrer Arbeitszeit nur noch die dienstlich benötigte Software verwenden. Vor allem erfüllen Klinik-Betreiber und Unternehmer durch den Schutz mit SecuLution die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Kurz: SecuLution reduziert Ausfälle, erhöht die Stabilität und Produktivität. Wie das im Einzelnen funktioniert, ist einfacher als man denkt. Für interessierte Administratoren und Manager hält SecuLution dazu eine ausführliche Online-Präsentation kostenlos bereit und bietet darüber hinaus die Möglichkeit einer kostenlosen 8-wöchigen Teststellung an. Sie haben so jederzeit die Möglichkeit, sich ein eigenes Bild über die Administration und die einfache Handhabung der Whitelist-Pflege zu machen.

Hier der schnelle Kontakt:
Telefon: (0 29 22) 95 89 – 21 0
Mail: info@seculution.com

Die einzelnen Features von SecuLution im Überblick:

- Application Whitelisting
- Device Whitelisting (USB)
- Device Encryption (USB Massenspeicher-Verschlüsselung, Data Leakage Protection DLP)
- Integrierte Agent Software-Verteilung
- Feingliedrige Rechtevergabe basierend auf Active Directory-Objekten, automatisiert (über Skripte)
- Integration in Netzwerküberwachungsanwendungen
- Cloud-basierter Whitelist-Verwaltungsservice