Whitelisting für Krankenhaus-Netzwerke

IT-Leiter: Ohne großen Aufwand ruhiger schlafen

Viele Unternehmen – auch im Gesundheitsbereich – setzten noch auf Antiviruslösungen der bekannten Virenhersteller. Eine Idee aus den 80er Jahren. Doch viel zuverlässiger als die Systeme auf schon bekannte Viren und Trojaner zu prüfen, ist das so genannte Whitelisting. Viele Krankenhäuser nutzen es schon. Nur was bekannt und sicher ist, kommt durch.

Ein kleiner Film im Internet demonstriert auf amüsante Art und Weise, um was es geht, wenn von „Whitelisting" die Rede ist. „Blacklisting", das machen die altbekannten Virenscanner.

„Das Leben ist nicht gerade einfach für IT-Administratoren", heißt es dort. Hacker wollen in das IT-Netzwerk einbrechen, Viren wollen die Systeme entern und sogar die eigenen Mitarbeiter versuchen manchmal, Dinge zu tun, die nicht nur nichts mit ihrer eigentlichen Arbeit zu tun habe, sondern die auch - oft aus Versehen - die Sicherheit der Unternehmens-IT gefährden können und die Systeme lahmlegen.

Ständig neue Bedrohungen

Für die IT-Leiter von Krankenhäusern bedeutet das: Heutzutage ist es viel einfacher, in ein Netzwerk einzubrechen, als es stabil am Laufen zu halten. Firewalls und Scanner für verbotene und potentiell gefährliche Inhalte sowie die guten alten Viren-Scanner aus den 80er Jahren sollen dabei helfen, das die IT ohne Probleme funktioniert. Doch die Bedrohungen nehmen zu – und ständig kommen neue, noch unbekannte hinzu. Die Virenscanner schauen sich jedes einzelne Programm genau an und entscheiden dann, ob es eine bekannte Gefahr darstellen könnte. Je nach dem wird Zugang gewährt - oder auch nicht. Doch allgemein gesagt, kommen Programme, die dem Scanner noch nicht als gefährlich bekannt sind, durch die Eingangstür. Das kann, wie jeder IT-Profi weiß, ein fataler Fehler sein. Doch dann ist es schon zu spät.

Malware verursacht in Unternehmen weltweit geschätzte Kosten von rund 500 Milliarden Dollar im Jahr. Jeden Tag kommen rund 25.000 neue Viren und andere Schädlinge in Umlauf. Professionell organisierte, kriminelle Banden legen mit so genannter (Erpresser)-Ransomsoftware Unternehmen lahm, was zur Existenzbedrohung führen kann.

Locky hat großen Schaden angerichtet

So hat der Krypto-Trojaner Locky, eine im Februar 2016 in verschiedenen Ländern, insbesondere in Deutschland, in Umlauf gekommene Schadsoftware, auch viele Krankenhäuser in Deutschland befallen. Etliche, so sagen Experten, haben tatsächlich auch Lösegeld an die Erpresser gezahlt, um wieder an ihre verschlüsselten Daten zu kommen.

Auch diejenigen, die nicht zahlten, hatten große finanzielle Schäden. Beim Lukaskrankenhaus in Neuss etwa lag der Schaden laut Geschäftsführer Nicolas Krämer im Zeitungsinterview mit der Neuss-Grevenbroicher Zeitung (NGZ) Anfang März 2016 bei einer Dreiviertel-Million Euro. „Jeder weitere Tag kostet 75.000 Euro. Aber wir versuchen das einzufangen", sagte Krämer.

Doch die Lösung dagegen ist ziemlich simpel, so dass man sich wundert, warum darauf nicht schon mehr Menschen gekommen sind. Das beschriebene Video zeigt sie: So wie man ja auch nicht jeden Menschen in sein Haus lässt, der bisher nicht als Krimineller aufgefallen ist, so funktioniert auch das Prinzip Whitelisting im Unternehmen. Wie Zuhause lässt man nur diejenigen Menschen – oder eben ausführbare Programme – zu sich hinein, die man schon kennt – und die als vertrauenswürdig gelten. In diesem Beispiel steht die eigene Wohnung für das Firmennetzwerk.

Alles das, was vom Whitelist-Filter nicht explizit als erlaubt eingestuft wird, kann der Anwender so gar nicht erst starten. Damit wird sämtliche Schadsoftware automatisch als unbekannt eingestuft und nicht ausgeführt, sie kann von daher auch keinen Schaden anrichten.

Ralf Plomann, Betriebswirt im Sozial- und Gesundheitswesen und IT-Leiter des St.-Marien-Hospitals in Lünen, war einer der ersten Kunden eines deutschen White-Listing-Anbieters. „Ich kann es jedem Krankenhaus empfehlen und stehe sehr gerne jedem IT-Leiter für Auskünfte zur Verfügung", sagt er. Vor einiger Zeit bekam er einen Anruf, bei dem ihm die Lösung empfohlen wurde. Nun läuft sie auf allen seinen rund 700 Geräten, an den zwei Krankenhäusern des Krankenhausverbundes St. Rochus, der angeschlossenen Schule und einem Weiterbildungsinstitut. Seine IT hatte seitdem noch nie ein Problem mit unerwünschter Software, sagt Plomann.

„Hoher Aufwand ist ein Irrglaube"

„Viele Administratoren glauben heute immer noch, dass der Schutz des Netzwerks durch Whitelisting mit einem hohen und nicht gerechtfertigten Aufwand verbunden ist. Doch das ist ein Irrglaube", sagt Plomann. Zumal auch die Anbieter das wissen und technisch alles tun, um mit diesem bekannten Vorurteil aufzuräumen.

Auch Volker Kliewe, EDV-Leiter des St. Elisabeth-Hospitals in Beckum, hatte diese Angst – bevor er seine Systeme mit Whitelisting schützte. „Ich war besorgt, dass die Erstellung und Pflege einer Whitelist der vertrauenswürdigen Anwendungen und Geräte sehr viel Arbeit ist. Aber es war dann überhaupt kein Problem, sondern in wenigen Arbeitsstunden

erledigt.“ Sein Fazit: „Das Schadsoftware-Problem betrachten wir bei uns als gelöst.“

Der Learning-Mode

„Alles per Hand zu pflegen, das wäre in der Tat sehr aufwendig. Doch die Administratoren können in der Erstkonfiguration ein „Golden Image“ benutzen, einen sicheren und sauberen Muster-Rechner, der die meisten Anwendungen enthält, die flächendeckend im Krankenhaus genutzt werden.

Alle dort vorhandenen Programme werden mit einem Klick eingelesen und in der Whitelist-Datenbank gespeichert. Auf diese Weise sind mit nur wenigen Schritte schon weit über 90 Prozent der benötigten Programme freigegeben. Der Rest wird durch den „Lernmodus“ erfasst. Das ist der besondere Trick, mit der die Integration nach nur wenigen Stunden Arbeit abgeschlossen ist. Software, die noch nicht in der Whitelist erfasst ist, Sonderfälle also wie Spezialsoftware, die nicht auf dem Musterrechner installiert war und daher in der Whitelist noch nicht enthalten ist, wird so automatisch gelernt.

In dieser Phase arbeiten die Anwender ganz normal weiter, das System erkennt unterdessen, dass auf der Liste noch das Abrechnungsprogramm einer kleinen Abteilung oder Individuallösungen wie das Analysetool für das Dialysegerät fehlen.Nachdem der Administrator den Lernmodus beendet hat, kann er mit Hilfe eines zentralen, Cloud basierten Dienstes den Grad der Vertrauenswürdigkeit der gelernten Programme prüfen. Jetzt und auch später können neue Programme auf Wunsch gegen die vom Hersteller zur Verfügung gestellte Liste bereits als sicher eingestufter Software abgeglichen werden.

Vertrauen von Null bis Zehn

Das System ordnet allen Programme Sicherheitslevels von Null bis Zehn zu, der IT-Verantwortliche muss sich also nur noch um die Programme kümmern, die ein unsicheres Trustlevel bescheinigt bekommen. Es bleiben erfahrungsgemäß nur noch wenige Anwendungen übrig, über deren Verbleib in der Whitelist der Administrator entscheiden muss, um so die Feinjustierung vorzunehmen. „Null“ sind etwa bekannte Trojaner, „Eins“ ist immer noch gefährlich, „Zwei“ bekommen Anwendungen wie ein Bitorrent-Client, „Drei“ unbekannte Programme. Alles im Bereich „Null“ bis „Zwei“ sollte als „nicht vertrauenswürdig“ grundsätzlich nicht in der Whitelist verbleiben und kann damit direkt aus dem Regelsatz gelöscht werden. Bei Programmen mit dem Trustlevel „Drei“ handelt es sich meist um Individualsoftware, für die weder klar ist, dass sie vertrauenswürdig ist, noch, dass sie es nicht ist, sodass der Administrator sich diese einmalig anschauen sollte.

Hashwert-Verfahren schützt vor Angriffen

Windows-Patches etwa gelten als vertrauenswürdig (Level Neun). Verglichen werden dabei jeweils die Hashwerte der Programme, sie sind den Programmen so eindeutig zuzuordnen wie der Fingerabdruck beim Menschen. Jeder Client, der eine Anwendung im Netzwerk ausführen möchte, gleicht diese Werte beim Starten mit der Positivliste der bekannten Fingerabdrücke der erlaubten Programme ab.

Ist der Wert unbekannt, bekommt der Anwender vor dem Start eine einstellbare Meldung, z.B.: „Bitte wenden Sie sich an Ihre EDV-Abteilung.“ Der Administrator kann den angegebenen Hashwert dann noch während des Anrufs mithilfe von Google oder TrustLeveldatenbanken prüfen - und das Programm gegebenenfalls an seiner Administratorkonsole live am Telefon frei schalten. Der dafür verantwortliche IT-Mitarbeiter sollte hier im Zweifelsfall natürlich genau kontrollieren, ob das Programm für die Arbeit wirklich notwendig und vertrauenswürdig ist – auch wenn die Anfrage vom Vorgesetzten oder dem Krankenhaus-Leiter kommt.

Die Vorzüge der Positivliste

„In meinen Augen ist das Whitelisting-Prinzip ein Beruhigungsmittel für Administratoren. Ich bin wirklich froh, mit dem System arbeiten zu können. Es erspart mir eine Menge Aufwand und gibt mir Zeit für andere Tätigkeiten“, sagt EDV-Leiter Kliewe aus Beckum. Und noch andere positive Nebeneffekte gibt es: Der IT-Leiter bekommt automatisch auch eine Übersicht über alle Programme. Während der Lernphase werden also auch Anwendungen entdeckt, die mit der Arbeit nichts zu tun haben oder Programme, die zwar teuer eingekauft, aber nie genutzt worden sind. Mit der Beschränkung der Internet-Nutzung hat das hier beschriebene Whitelisting übrigens nichts zu tun, es geht nur um ausführbare Programme, also zum Beispiel Anwendungen mit der Endung .exe.

Sogar Software von Geheimdiensten oder Angriffe, die so genannte Zero-Day-Exploits ausnutzen, würden so erkannt: Schwachstellen in der Software, die bösartig verwendet werden, bevor sie vom Hersteller geschlossen werden können.

Auch USB-Sticks werden geprüft

Das Prinzip geht aber noch weiter: Es gibt auch die Möglichkeit USB-Geräte auf die Whitelist zu setzen. So wird vermieden, dass sensible Daten von Rechnern im Unternehmen kopiert werden können. Ein nicht gelisteter USB-Stick wird von einem gesicherten Rechner nämlich einfach nicht erlaubt – eine logische Fortsetzung des Whitelisting-Gedankens.

„Für uns hat vor allem die Möglichkeit, auch USB-Geräte auf eine Whitelist setzen zu können einen unschätzbaren Vorteil. Wir müssen nicht alle USB-Ports einzeln sperren, sondern ermöglichen nur bestimmten Mitarbeiter diese Möglichkeit, per USB Daten auszutauschen“, sagt IT-Leiter Dirk Andrae, IT-Leiter des St. Joseph-Stifts Dresden.

Johannes Klostermeier