WEB-TIPP:
www.baramundi.de

Automatisierter Schutz vor Malware

Des einen Werkzeug ist des anderen Waffe

Informationen über mögliche Sicherheitslücken sind bei Cyberkriminellen ungefähr genauso beliebt wie Details über den letzten iPhone-Leak bei seinen Fans. Wird eine Schwachstelle in einer Software entdeckt, wird in Hackerkreisen nicht lange gemauschelt. Im Gegenteil: Angreifer im Netz bedienen sich regelmäßig an Schwachstellendatenbanken und tauschen sich in Foren über Lücken aus. Der nächste Exploit – also ein passendes Angriffswerkzeug – lässt sodann nicht lange auf sich warten.

Für IT-Administratoren bedeutet das: Vorsorge zur Verteidigung. Denn nur wer Schwachstellen im eigenen System frühzeitig entdeckt, versteht und behebt, erhöht die Sicherheit der Unternehmens-IT.

Allein in den letzten drei Jahren wurden laut National Vulnerability Database über 25.000 neue Sicherheitslücken registriert. Das sind über 150 neue Gefahren für Unternehmen und Anwender pro Woche. Und die Ausmaße sind mitunter immens: Mondelez, Beiersdorf und Maersk, um nur einige der bekanntesten Opfer des internationalen NotPetya-Angriffes zu nennen. Zum Retten der durch die Malware verschlüsselten Daten forderten die Angreifer ursprünglich ein Lösegeld von 100 Bitcoins – zum damaligen

Stand umgerechnet knapp 250.000€. Nicht nur für Opfer kleinerer Organisationen eine empfindliche Summe, sondern insbesondere auch ohne jegliche Garantie auf Einlösen des vagen Versprechens. Und auch wenn Sicherheitsexperten und -behörden vom Zahlen von Lösegeldforderungen grundsätzlich abraten, boomt die Schattenindustrie der Cyberkriminellen, die einzeln oder in Gruppierungen gebündelt im Verborgenen des Netzes ihr Geld verdienen.

Hundertprozentige Sicherheit gibt es nicht

Doch wo fängt man an, um den Angreifern Einhalt zu gebieten? Software selbst ist aufgrund seiner extrem hohen Komplexität nicht fehlerlos. Bei einer Software wie Windows mit Millionen von Zeilen Programmcode sind rein statistisch unzählige potenzielle Schwachstellen zu erwarten. Große Unternehmen wie Microsoft selbst sind sich dessen natürlich bewusst und engagieren häufig sogenannte White Hat Hacker zum proaktiven Auffinden dieser Lücken oder zahlen Prämien an die, die sie bereits entdeckt und dem Konzern gemeldet haben. Ist dies der Fall, stellen ordentliche Softwarehersteller den entsprechenden Patch – also die Lösung zur Behebung der Schwachstelle – schnell bereit. Für IT-Administratoren ist dies ein besonders kritischer Moment. Denn sobald Black Hat Hacker von der offiziellen Bereitstellung eines neuen Patches erfahren haben, setzen diese alles daran, auf Basis dessen, Rückschlüsse auf die ursprüngliche Schwachstelle zu ziehen und so schnell wie möglich ein entsprechendes Exploit zu erstellen, noch bevor die Lücke bei allen Anwendern geschlossen werden konnte. Völlige Sicherheit gibt es angesichts der Software-Komplexität und im Rennen gegen die Zeit also nicht. Was die IT-Administration deshalb nicht tun sollte: Den Schutz vor Malware auf die leichte Schulter nehmen oder sich selbst zu viel zumuten. Denn die Herausforderung alleine alle Sicherheitslücken auf den gesamten Rechnern, mobilen Endgeräten und Servern im Unternehmen im Blick zu behalten, ist schlichtweg nicht mehr zu stemmen. Auch steigt die Komplexität in IT-Abteilungen durch den Einsatz vieler unterschiedlicher Werkzeuge zur Überwachung und zum Management der Systeme.

Automatisierung schafft Zeit für Wesentliches

Die Bündelung eben dieser Werkzeuge in einer einzigen Oberfläche und die Automatisierung diverser Sicherheitsaufgaben entlastet und unterstützt den Administrator immens. baramundi bietet hierfür Lösungen zum Unified Endpoint Management (UEM). Unified Endpoint Management deshalb, da alle Clients über ein zentrales Tool ganzheitlich und einheitlich verwaltet werden. Das ist der erste Schritt zu mehr Sicherheit, denn nur wer einen genauen Überblick über all seine Ressourcen hat und deren Abhängigkeiten kennt, kann sie auch schützen. Ebenfalls unerlässlich und im UEM enthalten: eine Schnittstelle zu kontinuierlich aktualisierten Schwachstellendatenbanken anerkannter Organisationen, auf dessen Informationen die Lösung von baramundi zugreifen kann. So werden Schwachstellen auf Basis der Datenbanken automatisch erkannt und durch die Verteilung der entsprechenden Patches automatisiert behoben. Updates für häufig genutzte Anwendungen wie Adobe Reader, Java oder Firefox, verteilen Administratoren ebenfalls ganz einfach mit dem baramundi UEM. Dem Admin bleibt manuelles Durchsuchen eben jener Datenbanken, das Testen der eigenen Clients und das Durchführen und Kontrollieren der Patches – und damit sehr viel Zeit und Energie – erspart. In der Unternehmenslösung sind mittlerweile über 15.000 bekannte Schwachstellen eingepflegt, auf die die IT-Umgebung automatisiert gescannt wird. Admins können dabei nach Client, Schwachstelle und Gefährdungsgrad filtern und priorisieren: Was soll zuerst behoben werden – das Gerät mit den meisten Sicherheitslücken, die häufigsten Schwachstellen im System oder die gefährlichste Bedrohung? Eine Entscheidung, die der Administrator dann unter genauer Kenntnis seiner Umgebung und unter Berücksichtigung der eigenen IT-Prozesse zielsicher treffen kann.

Das Wissen über Schwachstellen ist für Hacker die Waffe, um mit dafür konstruierten Exploits die Sicherheitslücken auszunutzen. Für Administratoren ist dieses Wissen das Werkzeug, um die eigene IT-Umgebung zu prüfen und proaktiv mit Updates zu schützen.

Armin Leinfelder,
Leiter Produktmanagement
baramundi software AG

Nur die Kombination schafft Sicherheit

Je größer und ausgeklügelter der Schwarzmarkt für Exploits und Malware wird, umso intelligenter werden auch die Gegenmaßnahmen und Tools der Sicherheitsexperten. Der Trend zu entsprechenden Managementlösungen, die mithilfe automatisierter Prozesse wie dem Schwachstellenmanagement die Sicherheit der Unternehmens-IT unterstützen, ist nicht nur wegen der manuell unkontrollierbaren Masse an Clients notwendig, sondern schafft auch Zeit für wichtige Entscheidungen seitens des IT-Administrators. Denn hinter all den Zeilen an schädlichem Malware-Code sitzen Menschen, die unberechenbar agieren. Und diese gilt es mit den richtigen Werkzeugen, der stetigen Vorsorge, einem automatisierten Schwachstellenmanagement und der Expertise des Admins fernzuhalten.

Armin Leinfelder

Weiterführende Informationen: www.it-daily.net

Schwachstellenmanagement

Webinare