Mitarbeiter zählen zu den grössten Sicherheitsrisiken in Unternehmen

Mit IT-Security-Lösungen vorbeugen

Bei einem umfangreichen Phishing-Test in US-amerikanischen Krankenhäusern schätzten nur zehn Prozent der Mitarbeiter die Test-E-Mails mit Anhang als bedrohlich ein; alle anderen öffneten die Anhänge. Mittlerweile zählen Mitarbeiter zu den grössten Sicherheitsrisiken. Dabei gibt es längst IT-Security-Lösungen, die Attacken ins Leere laufen lassen.

Mitarbeiter von Unternehmen rücken immer mehr in den Fokus von Cyberattacken. Hacker versuchen so Zugriff auf die Ressourcen oder Daten von Unternehmen zu bekommen. Eine sehr beliebte Technik dabei ist es, Angestellten per E-Mail Schadsoftware unterzujubeln, die sich nach Ausführung dann im Unternehmensnetz breit macht und Löcher in die Abwehr des Unternehmens reisst.

Mitarbeiter sind beliebte Opfer

Angriffe mittels gefälschter E-Mails sind zwar schon altbekannt, haben aber in letzter Zeit an Brisanz gewonnen. So meldet Virenscanner-Anbieter Kaspersky, die Menge unerwünschter Mails sei im März 2016 auf fast 23 Millionen angestiegen – vier Mal mehr als im Monatsdurchschnitt von 2015. Bei dieser Häufung kann es an einem stressigen Arbeitstag leicht passieren, dass die als harmloser Anhang getarnte Malware vom Mitarbeiter ausgeführt wird. Sollte dann die Sicherheitssoftware den Schädling nicht erkennen, kann sich der Schadcode auf dem Client oder im Unternehmensnetz schnell ausbreiten.

Welch grosse Bedrohung gefälschte E-Mails für Unternehmen darstellen, musste auch der US-amerikanische Krankenhausbetreiber Atlantic Health System mit Sitz in New Jersey feststellen. Das Unternehmen hatte die Consulting-Firma CynergisTek aus Austin (Texas) für einen Phishing-Test beauftragt. Das Sicherheitsunternehmen verschickte im Auftrag des Krankenhausbetreibers an insgesamt 5000 Mitarbeiter manipulierte E-Mails, in denen es inhaltlich um Gehaltserhöhungen ging. Ergebnis des Tests war, dass gerade zehn Prozent der angeschriebenen Personen die Mail als verdächtig einstuften; alle anderen öffneten zumindest den Anhang und über die Hälfte von denen, die den Anhang öffneten, gaben darüber hinaus sogar persönliche Daten an.

Angriffe verhindern ist der beste Schutz

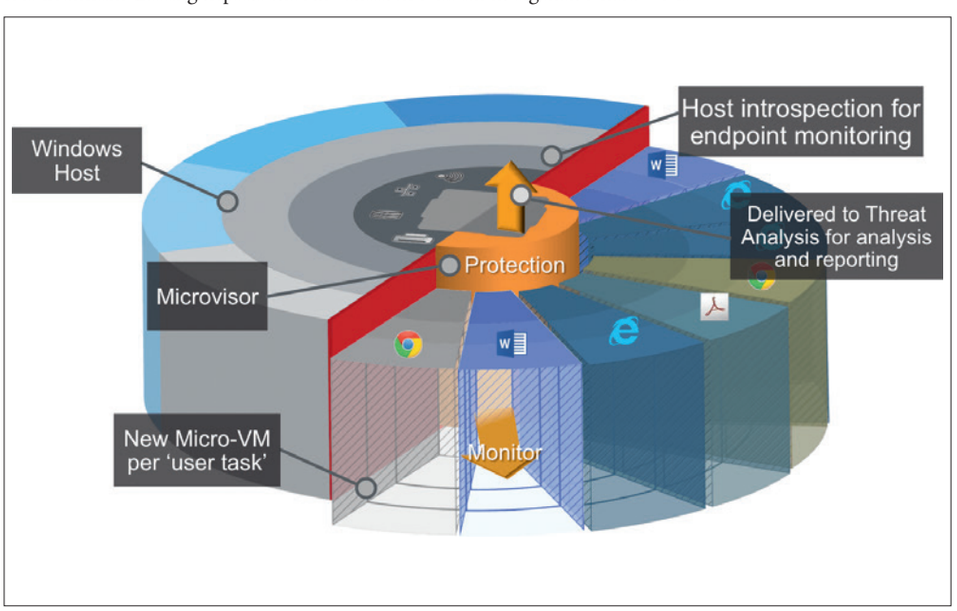
Der Test zeigt, dass sogar Menschen, die tagtäglich privat und beruflich mit dem Computer umgehen, nicht vor den raffinierten Tricks der Hacker gefeit sind. Genau an dieser Schwachstelle setzt die Sicherheitslösung von Bromium an, denn durch die Isolierung aller potenziell gefährlichen Prozesse in einer Micro-VM erreicht Malware nie das eigentliche Betriebssystem und kann somit weder lokal noch im Netzwerk Schaden anrichten, oder zu einem Datendiebstahl führen.

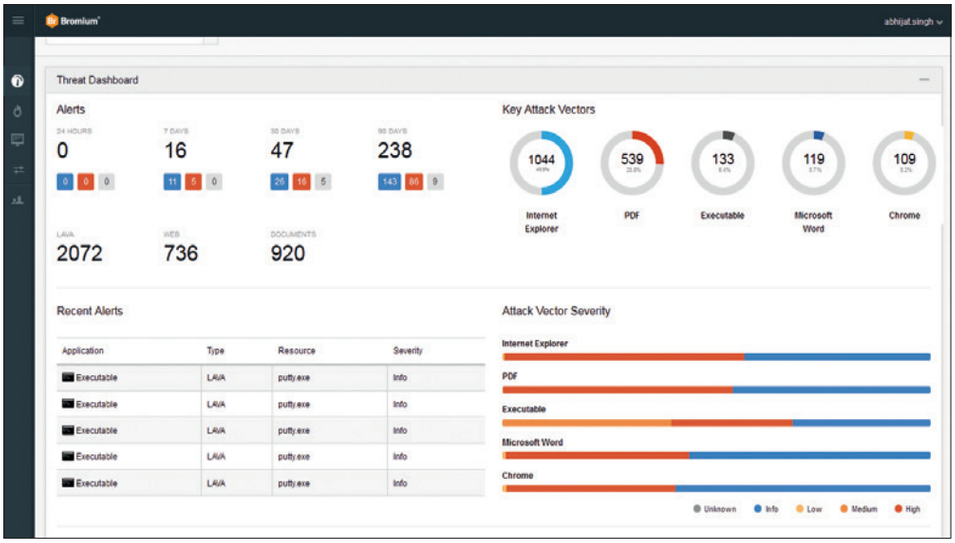
Auch Systeme, die beispielsweise nicht auf aktuellem Upgrade- oder Patch-Stand sind, bleiben damit umfassend geschützt.

Darüber hinaus macht die Lösung kein zeitaufwändiges und kostenintensives Neuaufsetzen von kompromittierten Rechnern erforderlich, da eine mögliche Schädigung auf die jeweilige Micro-VM beschränkt ist und diese automatisch

Jochen Koehler, Regional Director DACH, Bromium in Heilbronn

Die Bromium-Lösung kapselt alle Anwenderaktivitäten in eigenen Micro-VMs.





Das Dashboard des Bromium Enterprise Controller liefert einen detaillierten Überblick über den aktuellen Alarmierungsstatus.

nach Beendigung einer Aktivität, beispielsweise dem Schliessen eines Files oder Browser-Tabs, gelöscht wird; eine Ausbreitung von Schadcode ist damit ausgeschlossen. Nicht zuletzt bietet die Lösung den Vorteil, dass sie für den einzelnen Anwender im Hintergrund läuft, ohne dass er dabei Einschränkungen hinsichtlich Benutzerkomfort oder Systemperformance hat.

Micro-Virtualisierung ist zukunftsweisend

Weil die Mitarbeiter zunehmend ins Fadenkreuz von Hackern geraten, ist für die IT-Sicherheits-Experten in Unternehmen neuerdings die zentrale Frage, wie man solche Cyber-Attacken abwehren kann. Erfahrungsgemäss bietet klassische Sicherheitssoftware bei aktuellen Attacken meist nur einen begrenzten Schutz, da sie für die Abwehr Signaturen, Verhaltensanalysen oder heuristische Methoden nutzt. Da Hacker aber oft Techniken einsetzen, die noch nicht bekannt sind, versagt die traditionelle Sicherheitssoftware in vielen Fällen. Bromium verfolgt daher mit seiner Sicherheitslösung einen völlig anderen Ansatz, bei dem nicht die Erkennung von Schadcode im Mittelpunkt steht, sondern der Schutz davor, denn in der heutigen Zeit drehen sich die Sicherheitsfragen nicht mehr darum, ob das Netzwerk oder die Endpunkte kompromittiert werden, sondern wann.

Autor: Jochen Koehler ist Regional Director DACH bei Bromium in Heilbronn
Bilder: Bromium