Die Herausforderung

Die Kommunikation via E-Mail und der Zugriff auf das Internet sind alltäglicher Bestandteil unserer Arbeit. Traditionelle Sicherheits-Lösungen können die damit verbundenen Gefahren jedoch nicht zuverlässig bewältigen. So rückt das Endgerät immer stärker ins Blickfeld von Cyber-Kriminellen: Sie nutzen diese Schwachstelle massiv aus und stellen damit Behörden wie Unternehmen gleichermaßen vor ein Problem.

Das Problem

Für Angreifer ist es einfach, Schadcode durch minimale Veränderungen an Anti-Virus-Scannern und anderen erkennungsbasierten Sicherheits-Lösungen vorbei zu schleusen. Dabei sind die ***Anwender machtlos*** und merken oft erst, was passiert, wenn der Schaden bereits entstanden ist. Mitarbeiterschulungen im Umgang mit der Gefahr reichen nicht. Und E-Mails einfach nicht mehr zu öffnen oder dem Internet den Rücken zu kehren, ist natürlich auch keine Option. Was also tun, um sich vor den neuartigen Cyberbedrohungen zu schützen?

Die Lösung

Weil es unmöglich ist, Schadcode zuverlässig zu erkennen, empfiehlt sich ein Strategiewechsel: ***Isolation statt Detektion***, sprich die von Angreifern ausgehende Gefahr vom Endgerät und dem daran angeschlossenen Neztwerk fernzuhalten. Dieses Sicherheitsmodell wird vom BSI bereits seit mehreren Jahren empfohlen, weshalb viele Unternehmen und vor allem Behörden zum Surfen im Internet eine so genannte ReCoBS – Remote Controlled Browsers System – Umgebung aufgebaut haben und ihre Anwender über Terminal Server ins Internet verbinden. Sobald jedoch Dateien herunter geladen oder E-Mail-Anhänge geöffnet werden müssen, landet die darin versteckte Malware abermals auf dem Rechner und gegebenenfalls im Unternehmens- oder Behörden-Netzwerk. Die Bromium-Lösung ***Secure Platform*** zielt nicht nur auf den Browser als Sicherheitsschwachstelle ab, vielmehr werden damit alle potenziell gefährlichen Quellen auf dem Endgerät isoliert.

Das Produkt

Bromium Secure Platform schützt zuverlässig vor allen Schadcode-Angriffen über externe Schnittstellen am Rechner: Internet-Browser, E-Mails und USB-Zugänge sind für die Cyber-Kriminellen nicht mehr ausnutzbar, ihre Angriffe laufen ins Leere. Dabei greift Bromium das ReCoBS-Prinzip auf, isoliert jedoch Browserinhalte und Dateien direkt auf dem Endgerät. Die Lösungsmodule ***Secure Browsing*** und ***Secure Files*** können zusammen oder getrennt voneinander die beabsichtigte Schutzwirkung erzielen, indem alle potenziell gefährlichen Abläufe in so genannte Micro-VMs verlagert werden – das sind winzige, hoch performante, virtuelle Umgebungen, die bei Bedarf im Prozessor starten und einzelne Tasks voneinander wie auch vom Rechner selbst isolieren. So wird auch völlig unbekannter Schadcode für das Endgerät ungefährlich. ***Secure Monitoring*** beobachtet zusätzlich jede Aktion in einer Micro-VM auf ungewöhnliches Verhalten hin. Bei besonderen Auffälligkeiten erfolgt eine automatisierte Analyse, gefolgt von einer Meldung an den Anwender selbst oder an eine zentrale Überwachungsstelle für Sicherheitsvorfälle.