m-privacy White Paper

Titel	***Bromium* – ein Schutzsystem auf Basis lokaler Mikrovirtualisierung**	**Schlüsselwörter**	Mikrovirtualisierung, lokale Virtualisierung, Schutzsystem, ReCoBS
Autor	Patrick Leibbrand {p.leibbrand@m-privacy.de}	**Datum**	12.10.18
		Version	1.0

Inhalt

1 Einführung

Es gibt unterschiedliche Ansätze, Rechnersysteme und Netzwerke gegen Angriffe aus dem Internet zu sichern. Verbreitet sind Filtersysteme, die versuchen, Angreifer oder deren Verhaltensweisen zu erkennen und gefahrenträchtige Zugriffe automatisch zu unterbinden. Der prinzipielle Nachteil filternder Systeme ist die Tatsache, dass nur bekannte Bedrohungen zuverlässig erkannt werden und künstlich intelligente Mechanismen begrenzt zuverlässig sind. Fehlalarme bei zu restriktiver Filterung beziehungsweise schlechte Erkennungsraten bei unbekannten Schädlingen können die Folge sein. Vor diesem Hintergrund sucht man nach Möglichkeiten, Angriffe und Schadcode aus internen Netzwerken präventiv fernzuhalten, ohne deren Funktionalität durch tief eingreifende Sicherheitssysteme zu beeinträchtigen.

1.1 Lokale Virtualisierung als Sicherheitskonzept

Neben zertifizierbar sicheren, dedizierten Remote-Controlled Browser Systems (ReCoBS), die eine hardwaremäßig getrennte Ausführungsumgebung für potenziell gefährdete Applikationen wie den Webbrowser bereitstellen, erfreuen sich lokale Virtualisierungen einiger Beliebtheit. Hierbei werden Anwendungsprogramme direkt auf dem Rechner, auf dem sie laufen, in virtuellen Umgebungen gekapselt. Dabei bringen klassische Ansätze der lokalen Virtualisierungen ein rudimentäres Betriebssystem mit, in denen die abzusichernden Programme installiert sind. Härtungsmaßnahmen versuchen zu verhindern, dass Schadcode oder Angriffsaktivitäten aus der virtuellen Maschine „ausbrechen“ und den Hostrechner infizieren.

1.2 Mikrovirtualisierung mit *Bromium*

Neuere Entwicklungen verkleinern die virtuellen Umgebungen bis hinunter auf Applikationsebene. „Mikrovirtualisierung“ wird das Konzept genannt, dem beispielsweise das kommerziell erhältliche Schutzsystem *Bromium* folgt. Hierbei werden alle abzusichernden Programme innerhalb eines regulären Windows-Betriebssystems in separaten virtuellen Maschinen (VMs) gekapselt. Wird ein betreffendes Programm aufgerufen, startet die „Mikro-VM“ und führt die Zielapplikation aus. Für einen Anwender ist diese Art der lokalen (Mikro-)Virtualisierung transparent und im Normalfall unmerklich. Wird ein gesichertes Programm geschlossen, wird die betreffende Mikro-VM automatisch heruntergefahren und zurückgesetzt. Ein erneuter Start erfolgt idealerweise stets unter definierten Bedingungen. Mit einstellbaren Berechtigungen können die einzelnen Mikro-VMs gegeneinander sowie gegen das Betriebssystem des Hostrechners (Server oder Arbeitsplatz-PC) abgegrenzt werden.

2 Sicherheitsaspekte

Mikrovirtualisierung steht und fällt unter Sicherheitsaspekten einerseits mit der Sicherheit des verwendeten Hypervisors und andererseits mit der Qualität des Regelwerks, das die Berechtigungen der Mikro-VMs im System steuert und durchsetzt.

2.1 Microsoft Windows und Hyper-V als Systembasis

Bromium setzt auf Microsoft Windows auf und verwendet die systemeigene Virtualisierungstechnik Hyper-V, die unmittelbar auf Hardwarefunktionen der x64-Prozessoren von Intel und AMD zurückgreift. Die Praxis hat gezeigt, dass Hypervisoren ausnutzbare Sicherheitslücken enthalten. Entsprechende Hinweise sind Gegenstand der IT-Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI). Über solche Lücken kann das Hostsystem infiltriert werden, wodurch Angreifer möglicherweise Zugriff auf sensible Daten erhalten.

Im Fall von *Bromium* setzt auch der Control-Server auf Windows auf und nutzt zusätzlich eine herstellereigene SQL-Datenbank zur Verwaltung der Zugriffsregeln der Mikro-VMs innerhalb des Betriebssystems. Dies eröffnet weitere potenzielle Angriffsvektoren. Die Sicherheit der Virtualisierung hängt unmittelbar vom Betriebssystem ab, zusätzlich werden systemeigene Hilfsprogramme (SQL-DB) zur Verwaltung des sensiblen Regelwerks eingesetzt.

2.2 Eigensicherheit und Trennwirkung

Bei der Betrachtung von Schutzsystemen sollte der Blick nicht allein den primären Sicherheitsmerkmalen, sondern auch dem Selbstschutz und der Eigensicherheit des Systems im Fall einer Kompromittierung des eigentlichen Schutzmechanismus' gelten.

Bei lokalen Virtualisierungen stellt die virtuelle Umgebung die zentrale Hürde dar, darüber hinaus gibt es keine weiteren Barrieren zum Hostsystem. Dieser prinzipielle Nachteil tritt immer dann zutage, wenn sich Schutzsystem und zu schützendes System auf demselben physischen Rechner befinden. Die Trennung erfolgt rein softwaretechnisch und ist damit grundsätzlich leichter zu überwinden als eine hardwarebasierte Trennung von Ausführungsumgebungen auf unterschiedlichen physischen Rechnern.

Überdies machen Virtualisierungen mit Hyper-V von den Sicherheitsfunktionen Gebrauch, die durch die x64-Architektur bereitgestellt werden. Gravierende Schwachstellen der jeweiligen Prozessoren, die durch technisch hochstehende Angriffe wie Spectre oder Meltdown ausgenutzt werden, limitieren damit die Schutzwirkung aller Virtualisierungslösungen stark. Dies betrifft die klassischen Container mit eigener OS-Umgebung ebenso wie die beschriebene Mikrovirtualisierung.

2.3 Konzeptionelle Besonderheiten

Bromium virtualisiert Applikationen selektiv bei potenziell gefahrenträchtigen Operationen. Um Systemressourcen zu sparen, werden vertrauenswürdige Vorgänge dagegen nicht mikrovirtualisiert. Ein Download aus dem Internet etwa wird mit einer internen *Bromium*-Kennzeichnung versehen. So lange dieses „Untrusted-Flag“ erhalten bleibt, öffnet Bromium die heruntergeladene Datei mit virtualisierten Applikationen. Die Kennung kann jedoch durch vom Anwender veranlasste Dateioperationen verloren gehen. *Bromium* sieht diese Datei dann als unschädlich an, es erfolgt keine Mikrovirtualisierung beim Öffnen.

Vom Anwender selbst erstellte Dateien gelten unter *Bromium* generell als vertrauenswürdig. Werden Dateien aus unterschiedlichen Quellen zusammengeführt, erfolgt keine Unterscheidung hinsichtlich der Vertrauensstufe. Für den Anwender ist nicht ersichtlich, ob er eine sichere Bilddatei oder eine mit einem Makroschädling behaftete Tabelle in sein Textdokument einfügt. *Bromium* unterbindet die Handhabung unsicherer Inhalte nicht. Die spezifische Kennzeichnung ist in applikationseigenen Dateibrowsern nicht mehr sichtbar.

Mitverantwortung des Anwenders

Sicherheit und Anwenderfreundlichkeit sind bei *Bromium* letztlich Gegenstand eines sachgerecht auszuhandelnden Kompromisses. Die meisten Zugriffsanforderungen werden per definitionem in „vertrauenswürdig“ und „nicht vertrauenswürdig“ unterteilt. Diese Unterscheidung kann jedoch durch einfache Benutzeraktionen aufgehoben werden. Dann unterbleibt die trennende Mikrovirtualisierung von *Bromium*. Damit liegt ein erheblicher Teil der Verantwortung für das Sicherheitsniveau des Gesamtsystems beim Anwender. Dies kann gegenüber der zwangsläufigen Wirksamkeit eines vorgeschalteten Schutzsystems einen praxisrelevanten Nachteil darstellen.

Virtualisierungskonzept mit Ausnahmen

In diesem Zusammenhang soll nicht übersehen werden, dass nicht alle Anwendungsprogramme im Windows-System durch *Bromium* mikrovirtualisiert werden. Manche Applikationen, auch solche mit Internetzugang, sind hiervon explizit ausgenommen. In diese Kategorie gehören beispielsweise Virenscanner. Diese Art filternder Schutzprogramme fällt immer wieder durch schwerwiegende Sicherheitslücken auf. Angreifer können sich die hohen Systemberechtigungen des Virenscanners aneignen und sich unbehelligt im Hostsystem bewegen. Die sicherheitstechnische Bewertung von *Bromium* kann dies negativ beeinflussen, zumal entsprechende Angriffe nicht hypothetisch sind.

2.4 Fazit: Sicherer als Windows allein – schwächer als ReCoBS

Insgesamt betrachtet liegt die Systemsicherheit etwas über dem Niveau eines Windows-Systems ohne Virtualisierung. Die systemeigenen Sicherheitsmechanismen werden zwar bestmöglich genutzt, eine sicherheitstechnische „Härte“ eines kernbasierten Zugriffskontrollsystems für Programme und Prozesse nach dem Vorbild von RSBAC (Rule-Set Based Access Control) lässt sich jedoch nicht erreichen.

3 Verwaltungsaspekte

Bromium kapselt Applikationen im Windows-Betriebssystem in Mikrovirtualisierungen und versieht diese mit einem komplexen Geflecht aus Berechtigungen. Diese Berechtigungen sind sowohl funktions- als auch sicherheitsentscheidend. Die notwendigen Regelsätze für Standardprogramme unter Windows stehen bereits mit dem Erwerb der Software zur Verfügung. Für anwenderspezifische oder weniger verbreitete Programme müssen die Berechtigungen gesondert zusammengestellt und konfiguriert werden. Aufgrund der Komplexität sind mitunter längere Implementierungsphasen und eingehende Tests unvermeidlich.

Bromium kann ausschließlich auf Arbeitsplatzrechnern („Fat Clients“) im Sinne einer Endpoint-Security-Lösung verwendet werden. Der Einsatz in Verbindung mit Terminalservern ist nicht möglich. Terminalserver gelten jedoch als besonders schutzbedürftig, da ihr Ausfall infolge von Angriffen oder Schadcodebefall in der Regel erhebliche Auswirkungen hat. Die Festlegung von *Bromium* auf Endgeräte kann in großen Infrastrukturen mit IT-Zentralversorgung (Nutzung von „Thin Clients“) einen gravierenden Nachteil darstellen.

Bromium agiert auf Endgeräten flexibel und performant, bewegt sich jedoch im Spannungsfeld von Sicherheit, Funktionalität und Komplexität. Zum robusten Betrieb des Schutzsystems in verteilten, heterogenen Systemumgebungen bedarf es einer leistungsstarken Systemadministration sowie in der Regel erweiterter Serviceleistungen durch den Hersteller. Auch in Anbetracht der kurzen Update-Zyklen vieler verbreiteter Applikationen wie beispielsweise Webbrowsern ist beim Einsatz von *Bromium* mit erhöhtem Aufwand respektive Wartezeiten bis zur Freigabe durch den Hersteller zu rechnen.

4 Zusammenfassung

Bromium bietet ein Sicherheitsniveau auf einem für lokale Virtualisierungslösungen üblichen Level. Es ist einerseits für den Anwender bei korrekter Konfiguration weitgehend transparent, andererseits administrativ ausgesprochen komplex. Das Schutzsystem kann jenseits der herstellerseitig unterstützten Applikationen mit entsprechendem Aufwand auf andere Anwendungsprogramme angepasst werden. Das Verhältnis zwischen Funktionalität und Sicherheitszugewinn ist ausgewogen. Nachteilig wirkt sich aus, dass ein Teil der Verantwortung für die erreichbare Systemsicherheit jedoch beim Anwender verbleibt. Weiterhin ist *Bromium* nur auf Arbeitsplatzrechnern („Fat Clients“) einsetzbar, nicht jedoch in Terminalserver-Umgebungen.

Bromium sichert nicht nur stark gefährdete Applikationen wie den Webbrowser. Auch Office-Programme und verschiedene E-Mail-Systeme können damit isoliert werden. Diese Vielseitigkeit hebt *Bromium* von anderen lokalen Virtualisierungen ab. Zusätzlich bietet *Bromium* dem Administrator durch Visualisierung erkannter Angriffsversuche erweiterte Analyseoptionen und eröffnet gezielte Interventionsansätze.

Allerdings handelt es sich bei *Bromium* nicht um ein Remote-Controlled Browser System (ReCoBS) im technischen Sinne. Ein Webbrowser wird in *Bromium* zwar zur Laufzeit softwaremäßig abgeschottet, aber nicht in einer externen Laufzeitumgebung auf einem dedizierten Rechner ausgelagert. Damit fehlt die sichere Netzwerkverbindung als zusätzliche Barriere. Stattdessen ist der Browser lokal auf dem Arbeitsplatzrechner erreichbar, unterliegt jedoch dem Regelwerk der ihn umgebenden Mikro-VM. Die Trennwirkung von *Bromium* ist daher mit der eines dedizierten ReCoBS nicht vergleichbar. Auch administrativ sind vorgeschaltete Schutzsysteme nach dem ReCoBS-Prinzip einfacher zu handhaben. Sie kapseln jedoch neben dem Browser nur wenige weitere Applikationen.

5 Alternativen

Bromium erfordert in typischen Infrastrukturen einen relativ hohen initialen Aufwand für Installation, Konfiguration und Test. Auch im Produktivbetrieb sind regelmäßige Nacharbeiten zu erwarten, beispielsweise bei Aktualisierungen der Zielapplikationen. Die Schutzwirkung von *Bromium* übersteigt dabei nicht die Leistung anderer Virtualisierungstechniken.

Risikobasierter Ansatz

Ein risikobasierter Ansatz kann helfen, Aufwand und Kosten zu kontrollieren. So eignet sich ein dediziertes ReCoBS als Alternative zu *Bromium*, um den besonders gefährdeten Webbrowser sowie ausgewählte, unter hohem Angriffsdruck stehende E-Mail-Konten zuverlässig zu sichern. Für Office-Anwendungen, regulären E-Mail-Verkehr und Spezialanwendungen reichen mitunter sorgfältige Konfiguration und klassische Filtertechniken für ein angemessenes Schutzniveau aus. Letztere sind im Netzwerk oft ohnehin vorhanden und sollten beibehalten werden.

Die kombinierte Vorgehensweise reduziert die Komplexität der Sicherheitsarchitektur deutlich und vermindert insbesondere den administrativen Ressourcenbedarf. Zugleich werden hochfrequentierte Einfallstore bestmöglich geschlossen. Technisch versierten Angriffstechniken wie beispielsweise Meltdown oder Spectre begegnen dedizierte ReCoBS wirkungsvoller als jede lokale Virtualisierung, die sich allein auf die Sicherheitsfeatures der lokalen Hardware verlässt.

6 Weiterführende Informationen

- **Internetpräsenz der m-privacy GmbH**
  https://www.m-privacy.de

7 Unternehmensprofil

Die m-privacy GmbH mit Sitz in Berlin entwickelt TightGate-Pro, eine Client-Server-Lösung zur sicheren Internetanbindung von Computerarbeitsplätzen nach dem Prinzip des ferngesteuerten Webbrowsers. TightGate-Pro ist auch in einer BSI-zertifizierten Version erhältlich und erreicht die Schutzstufe EAL3+. Darüber hinaus stellt das Unternehmen ein umfangreiches Dienstleistungsportfolio zur IT-Sicherheit und zum Datenschutz für professionelle Anwender bereit.