Browser als Einfallstor für Cyberangriffe

Mit proaktivem Ansatz Sicherheit nachhaltig implementieren

ROHDE&SCHWARZ
Cybersecurity

Browser in the Box

White Paper | Version 01.01

Kurzdarstellung

Situation

Cyberangriffe werden komplexer und kosten Unternehmen Milliarden

Das Internet mit Milliarden von Nutzern und unbegrenzter Rechenleistung ist das mächtigste Netzwerk aller Zeiten. Da ist es nicht verwunderlich, dass es auch kriminelle Aktivitäten evoziert. Laut einer Studie des Bitkom sind zwei Drittel der Industrie bereits betroffen, der Schaden in Deutschland wird auf 55 Mrd. Euro pro Jahr geschätzt.[1] Neben nicht erfolgten System- oder Softwareupdates ist besonders der Browser das Einfallstor für Viren, Trojaner, Ransomware, Advanced Persistent Threats und Zero-Day-Exploits.

Problem

Internet Explorer, Firefox, Chrome und Co. – Das Surfen im Internet als Schwachstelle

Es ist in der Tat so, dass ein Großteil der Schadsoftware heute über einen Browser bzw. die besuchte Webseite in das Netzwerk gelangen.[2] Problematisch sind dabei vor allem aktive Inhalte wie Flash, Java, JavaScript, ActiveX oder HTML 5. Dabei wird fremder, externer Code auf dem PC, auf dem eigenen Betriebssystem und damit in der Dateninfrastruktur ausgeführt. Enthält dieser Programmcode Schadsoftware, so gelangt diese ebenfalls zur Ausführung. Dazu gehören auch E-Mails mit schadhaften Links, die im Browser geöffnet werden und dann zu destruktivem Verhalten auf dem PC und im Netzwerk führen.

Lösung

Trennung von Intranet & Internet durch Zwei-Browser-Strategie

Der entscheidende Punkt ist: Das Fundament für funktionierende Cybersicherheit muss neu gegossen werden. Das manifestiert sich bei Rohde&Schwarz Cybersecurity mit dem Ansatz „Security by Design“ und wird unter anderem mit dem Produkt Browser in the Box umgesetzt. Das Grundprinzip ist hier, dass Betriebssystem und Browser komplett voneinander getrennt werden. Der Browser selbst ist in einer virtuellen Maschine eingekapselt. So wird Schadsoftware vom PC und der Dateninfrastruktur des Nutzers bzw. dem Unternehmensnetzwerk ferngehalten. Hier läuft dann jeder Aspekt einer Webseite – wie Bilder, Werbebanner, Texte, Videos – in einer eigenen Enklave, ohne das Betriebssystem oder die Dateien zu beeinträchtigen.

Resultat

Hohe Nutzerakzeptanz beim Surfen im Internet und gleichzeitig hohe Sicherheit für das Netzwerk

Wichtig ist, dass Mitarbeiter nun jederzeit sicher im Internet surfen können. Eine große Gefahrenquelle ist somit beseitigt. Ganz wichtig: Für die Nutzer gibt es keine Einschränkung bei der Internetnutzung. Für Unternehmen bedeutet der flächendeckend sichere Internetzugang eine erhebliche produktive und finanzielle Entlastung. Denn weniger gehackte PCs reduzieren die Ausfallzeiten von IT-Systemen und damit einhergehende Produktivitätseinbußen. Natürlich ist das alles auch eine Erleichterung für die IT-Administration, die sich nicht mehr mit langwierigem Neuaufsetzen von PCs beschäftigen muss.

[1] Berg, Achim: Wirtschaftsschutz in der digitalen Welt (2017), https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017-v5.pdf (Stand: 14.08.2017)

[2] Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI für Sichere Web-Browser, https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards/Sichere_Web-Browser/Sichere_Web-Browser_node.html (Stand 20.09.2017)

Inhaltsverzeichnis

1 Cyberkriminalität: Das Internet als Gefahrenschwerpunkt

Seitdem es Datennetzwerke gibt, wurden diese ausgenutzt und kompromittiert. Heutzutage ist das Internet mit Milliarden von Nutzern und unbegrenzter Rechenleistung das mächtigste Netzwerk aller Zeiten. Da ist es nicht verwunderlich, dass es nun auch in den Fokus von Kriminellen gerückt ist. Locky Anfang 2016, Goldeneye Ende 2016, WannaCry im Mai 2017 und der Wiper NotPetya – basierend auf Petya – im Juni 2017 sind die bisherigen Höhepunkte einer Cyberangriffswelle. Für Unternehmen ist diese Entwicklung bedenklich. Der Schaden, welcher deutschen Unternehmen durch Plagiate und den Verlust der Wettbewerbsfähigkeit in Folge von Cyberangriffen entsteht, beläuft sich laut einer Studie des Bitkom auf 55 Milliarden Euro[3] – dieser ist wohlgemerkt in einem einzigen Jahr entstanden. Global liegt der Schaden bei 416 Milliarden Euro.[4] Hinzu kommt der zunehmende finanzielle Verlust durch Ransomware: Kriminelle kapern Daten und erpressen den Eigentümer. Es ist an der Zeit, die digitale Sorglosigkeit zu verlieren. Gleichzeitig sind Unternehmen aber gut beraten, sich nicht durch Angst und Panik verunsichern zu lassen. Die Gefährdung ist da, jetzt kommt es darauf an, diesen mit neuen Ansätzen und Lösungen entgegenzutreten.

1.1 Was ist die größte Schwachstelle im Unternehmensnetzwerk?

Um diese Frage ganz kurz und knapp zu beantworten: Es ist der Mensch selber. Bei 62% der von Wirtschaftsspionage, Sabotage und Datendiebstahl betroffenen Unternehmen war ein Mitarbeiter das Einfallstor.[5] Die E-Mail ist als Gefahrenpunkt schon bekannt. Durch die jüngsten Cyberangriffe wurde ebenfalls deutlich, dass ausbleibende System- oder Softwareupdates ebenfalls ein Schwachpunkt sind. Weniger bekannt ist, dass besonders der Browser als Einfallstor für Schadsoftware ausgenutzt wird. Es ist in der Tat so, dass ein Großteil aller Cyberangriffe heute über einen Browser bzw. die besuchte Webseite erfolgen.[6] Google selber stuft mindestens 10.000 Seiten täglich als unsicher ein.[7] 60% davon verbreiten Schadsoftware. Die restlichen 40% werden für Phishing-Angriffe benutzt.

Das Surfen auf Webseiten ist ein integraler Teil in der alltäglichen Arbeitsroutine. Dem stehen aber die ständig wachsenden Gefahren von diesen Angriffen gegenüber. Problematisch sind dabei vor allem aktive Inhalte wie JavaScript, Java, ActiveX, Flash oder HTML 5. Diese Programmierschnittstellen erlauben den Zugriff auf den PC des Nutzers, also auf das Datei- oder Betriebssystem. Trojaner, Viren oder Würmer können damit diese Schnittstellen zum Zugriff auf vertrauliche Daten missbrauchen. Ganz konkret ist es dann so, dass fremder, externer Programmcode auf dem PC mitten auf dem eigenen Betriebssystem und damit der Dateninfrastruktur ausgeführt wird. Enthält dieser Programmcode Schadsoftware, so gelangt diese ebenfalls zur Ausführung. Dabei geschieht die Ausführung der aktiven Inhalte bereits beim Laden der Webseite, ohne weitere Interaktion. Somit besteht schon beim Ansehen von Webseiten die Gefahr der Infektion mit Schadcode.

---

[3] Berg, Achim: Wirtschaftsschutz in der digitalen Welt (2017), https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017-v5.pdf (Stand: 14.08.2017)

[4] Jansen, Jonas: Cybersicherheitspersonal gesucht (2017), http://blogs.faz.net/netzwirtschaft-blog/2017/02/17/cybersicherheitspersonal-gesucht-4024/ (Stand 12.08.2017)

[5] Bitkom e.V.: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie (2016), https://www.bitkom.org/noindex/Publikationen/2016/Studien/Spionage-Sabotage-und-Datendiebstahl-Wirtschaftsschutz-in-der-Industrie/161110-Studie-Wirtschaftsschutz.pdf (Stand 23.07.2017)

[6] Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI für Sichere Web-Browser, https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards/Sichere_Web-Browser/Sichere_Web-Browser_node.html (Stand 20.09.2017)

[7] Beiersmann, Stefan: Transparenzbericht. Google nennt erstmals Statistik zu gehackten Websites http://www.zdnet.de/88159856/transparenzbericht-google-nennt-erstmals-statistik-zu-gehackten-websites/ (Stand 14.08.2017)

2 Bisherige Ansätze der Bedrohungsabwehr

Die bisherigen Ansätze in der Bedrohungsabwehr waren rein reaktiver Natur. Zu dieser Art von Abwehrdesign zählen z.B. die Antiviren-Softwareprogramme. Diese werden dem stetig wachsenden Bedrohungsszenario aber nicht mehr gerecht. Die Logik dieser Programme erfolgt nach dem Blacklisting-Verfahren. Hiermit werden lediglich bereits bekannte Bedrohungen abgewehrt. Dies ist auch unter dem Begriff Pattern-Matching bekannt und „dient nur noch dazu, dass Grundrauschen und ältere Gefahren fernzuhalten."[8] Zero-Day-Exploits, die bisher unbekannte Sicherheitslücken ausnutzen, bleiben so unentdeckt und werden von Antivirenprogrammen nicht herausgefiltert.

Wenn es konkret um die Internetnutzung in Unternehmen geht, kann man durch restriktive Ansätze versuchen, die Gefahren einzudämmen.

Hier sind dazu ein paar Beispiele dazu:

- Es werden nur dezidierte Rechner für den Internetzugang zur Verfügung stellt. Diese haben keine Anbindung an das Intranet und stehen isoliert vom Netzwerk zur Verfügung. Einschränkung: Aufgrund des integralen Bestandteils des Internets im Arbeitsalltag ist das kein praktikabler Ansatz mehr.

- Den Zugang zum Internet wird nur mit reduziertem Funktionsumfang zur Verfügung gestellt. Das würde unter anderem bedeuten, dass aktive Inhalte abgeschaltet werden. Einschränkung: Ein Großteil der Webseiten wäre nicht aufrufbar. Der Webbrowser läuft auf einem Terminal Server. Der Zugriff erfolgt auf dem PC via Desktop-Viewer. Einschränkung: Aufwändiges Recovery des betroffenen Terminal Servers nach Befall durch Schadsoftware. Dabei ist nicht immer klar, ab welchem Zustand der Terminal Server überhaupt aufwändig zurückgesetzt werden muss. Hinzu kommt eine hohe Auslastung der Netzwerkbandbreite. Gleichzeitig ist die Skalierung bei vielen Nutzern ungünstig, gerade wegen der Bandbreitenbelastung. In diesem Szenario ist zudem die Nutzung von Hotspots und anderen, nicht firmeneigenen WLANs, nicht möglich.

- Schutz des Internetzugriffs durch Proxy-Server/Firewall in eigener DMZ. Einschränkung: Wie effektiv dieser Schutz ist, hängt maßgeblich von der Erkennungsrate des Proxies für Schadsoftware ab. Für bereits bekannte Schadsoftware ist es effektiv, hat aber ihre Grenzen, wenn es um neue Gefahren geht. Beim Herausfiltern von aktiven Inhalten steht man in einem ständigen Spannungsfeld von Bedienbarkeit und Sicherheit.

Alle diese Ansätze haben mitunter ihre Berechtigung, aber: Die Arbeitsfähigkeit der Mitarbeiter ist aufgrund schlechter Bedienbarkeit stark eingeschränkt. Darunter leidet letztendlich die Produktivität und das ist aus Unternehmenssicht, trotz vermeintlich gestiegener Sicherheit, kein lohnenswerter Ansatz. Gleichzeitig ist bei diesen Ansätzen der Schutz vor unbekannten Angriffen nicht grundsätzlich gelöst.

[8] Schlede, Frank-Michael (2017): Smart-Security-Lösungen schlagen Malware. Cyberangriffe werden immer ausgefeilter. So halten Unternehmen damit Schritt. In: com! Professional, 2017, 07, S.96 - 100

3 Paradigmenwechsel durch proaktive Sicherheit

Damit sich Unternehmen vor den heutigen Gefahren aus dem Netz schützen können, ist ein Paradigmenwechsel nach dem Ansatz „Security by Design“ angebracht. Dieser beinhaltet eine Abkehr von reaktiven, hin zu proaktiven Lösungen. Dieser grundlegende Wandel ist vergleichbar mit der Entwicklung der Sicherheitssysteme in der Automobilindustrie: Airbags alleine reichen für den Schutz der Insassen bei Unfällen nicht mehr aus. Vielmehr sollte vermieden werden, dass es zu Unfällen mit gefährlichen Aufprällen kommt. Um Vorfälle nicht nur zu lindern, sondern ganz zu verhindern, wurde das Elektronische Stabilitätsprogramm (ESP) eingeführt. Eine solche proaktive Technologie wird auch in der IT-Sicherheit benötigt.

Beispiele für proaktive Technologien lassen sich in folgende zwei Hauptbereiche mit den entsprechenden Unterbereichen aufteilen:

1. **Separation, Integritätsprüfung**
   - Separation kritischer Bereiche in voneinander isolierte Komponenten
   - Reduzierung der sicherheitsrelevanten Komponenten Trusted Computing Base (TCB)
   - Integritätsschutz der Komponenten
   - Datenaustausch nur über klar definierte Schnittstellen
   - Technologien: Virtualisierung, gehärtete Sicherheitskerne

2. **Next-Generation-Firewalls mit Whitelisting**
   - Nur bekannte, validierte Protokolle werden zugelassen
   - Nicht zuzuordnende Pakete werden abgewiesen
   - Technologien: Deep Packet Inspection Engine

Reaktiver Ansatz: „Airbag-Methode“ – „Wenn‘s passiert, soll‘s weniger wehtun.“ (Foto: © istockcom | 3alexd)

Proaktive IT-Sicherheit: „ESP-Strategie“ – Verhindern, dass man überhaupt ins Schleudern kommt. (Foto: © istockcom | mevans)

4 Sicher im Internet mit Browser in the Box

„Security by Design“ manifestiert sich in unserem Produkt Browser in the Box. Das Grundprinzip ist hier, dass Betriebssystem und Browser komplett voneinander getrennt werden. Der Browser selber ist in einer virtuellen Maschine eingekapselt. So wird Schadsoftware vom PC und der Dateninfrastruktur des Nutzers ferngehalten. Jeder Aspekt einer Webseite, wie Bilder, Werbebanner, Texte oder Videos läuft in ihrer eigenen Enklave, ohne das Betriebssystem oder Dateien zu beeinträchtigen. Die Lösung wurde im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) für den Einsatz in Behörden entwickelt. Browser in the Box z.B. wird bereits von der Polizei in Baden-Württemberg eingesetzt. Die Mitarbeiter in den Polizeidienststellen nutzen Browser in the Box bei Ermittlungen im Internet oder bei der Recherche auf einschlägigen und mitunter nicht vertrauenswürdigen Webseiten. Sie können das Internet dabei ohne Beeinträchtigungen nutzen, während Browser in the Box im Hintergrund läuft.

4.1 Trennung von Intranet & Internet durch Zwei-Browser-Strategie

Der Ansatz von Browser in the Box begründet sich in einer Zwei-Browser-Strategie, die das Intranet und Windows-Betriebssystem vom Internet trennt. Dieser proaktive Ansatz geht davon aus, dass Webseiten im Internet potenziell gefährlich für den PC und das Unternehmensnetzwerk sein können bzw. dass eine hundertprozentige Sicherheit nicht erreicht werden kann. Eine komplette Isolierung der beiden Systeme ist also erforderlich. Ergo, selbst wenn ein einzelnes System kompromittiert wird, ist nicht das gesamte Unternehmensnetzwerk gefährdet. Browser in the Box ist vom Windows-Betriebssystem und vom Intranet vollständig isoliert und läuft in einer virtualisierten Umgebung. Es wird kein gemeinsamer Speicher und Kernel mehr geteilt, wie es z.B. beim Sandboxing der Fall wäre.

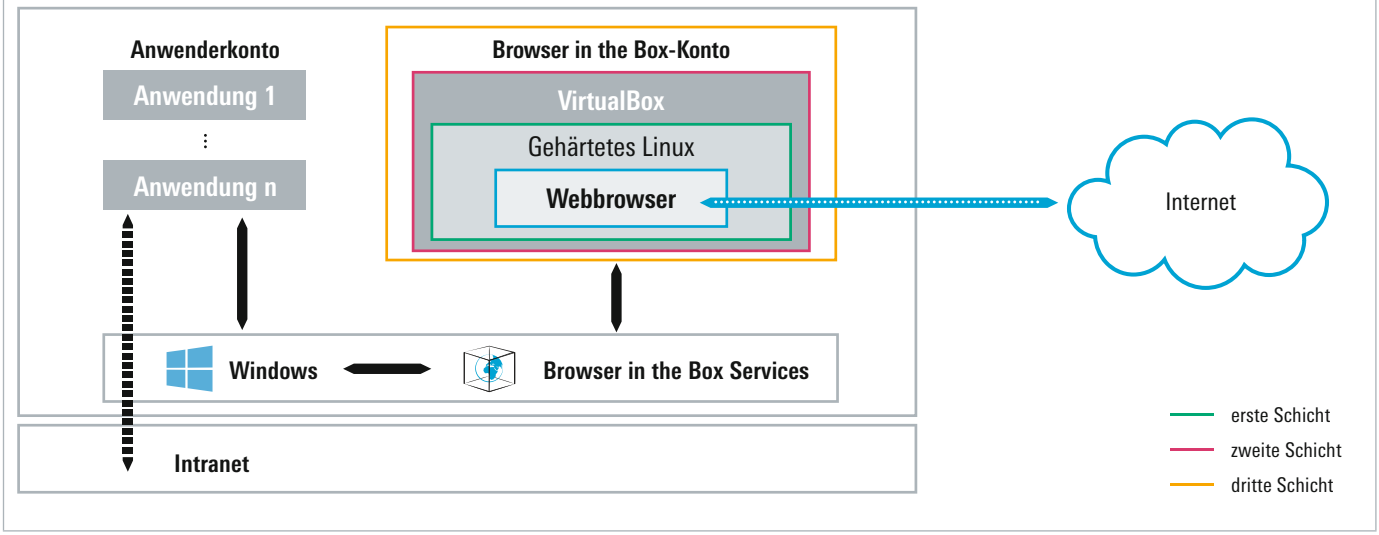
Funktionsweise und technisches Set-up

Bei Browser in the Box gehören drei Isolationsschichten zum Sicherheitskonzept:

- Die erste Schicht ist ein gehärtetes Linux mit AppArmor Whitelisting.
- Die zweite Schicht ist die Vollvirtualisierung mit der OpenSource-Software VirtualBox.
- Die dritte Isolationsschicht ist ein separater, nicht-interaktiver und eingeschränkter Windows-Benutzerkontext.

Bei dem gehärteten Linux hat man es mit einem minimalisierten Betriebssystem zu tun, auf dem nur der Browser und keine anderen Anwendungen ausgeführt werden. Hierbei wird der Kernel um das AppArmor-Whitelisting erweitert. Mit Hilfe von AppArmor wird anschließend auf Prozessebene festgelegt, welche Zugriffe innerhalb des virtualisierten Linux erlaubt sind. Führt eine Anwendung

Abbildung 1: Isolation auf Rechnerebene



im Browser eine unerlaubte Operation aus, da diese Anwendung beispielsweise von einem Angreifer manipuliert wurde, wird dem Prozess der Zugriff auf diese Operation untersagt. Im Vergleich zu alternativen Lösungen werden Speicher und Kernel für die Verwendung von Browser in the Box nicht mit dem Windows-Hostsystem geteilt. Durch den zusätzlichen Einsatz von Linux schafft man Diversität, die einem zusätzlich Vorteile verschafft. Denn ein Angriff müsste auf Linux UND Windows ausgelegt sein. Damit steigt für potenzielle Angreifer der Aufwand erheblich, wobei in der Folge die Angriffswahrscheinlichkeit abnimmt.

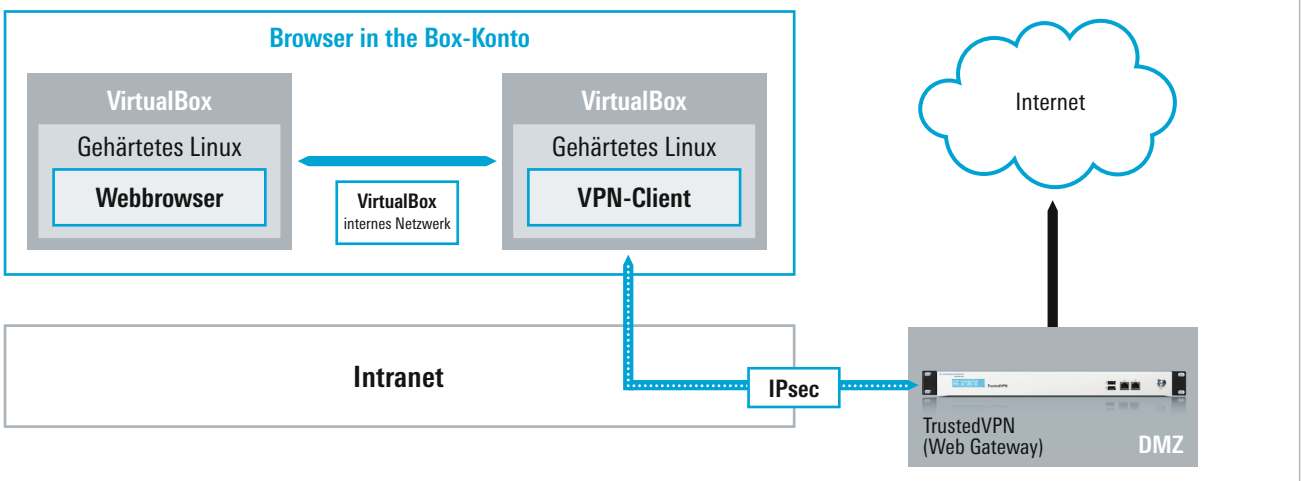
Wie schon weiter oben erläutert, kommt bei Browser in the Box durch die verschiedenen Isolationsschichten die Separation und das Whitelisting als proaktive Sicherheitsstrategien ganz klar zum Tragen. Statt eines zusätzlich isolierten physikalischen PCs für das Surfen im Internet wird ein virtueller PC auf dem normalen Arbeitsplatz-PC erzeugt. Während die Anwendungen des Benutzers direkt im Betriebssystem ausgeführt werden, wird der Browser in einer virtuellen Maschine innerhalb eines gehärteten Linux ausgeführt. All diese Komponenten haben keinen Zugriff auf die Hardware oder auf das Windows-Hostsystem, sondern lediglich auf die virtuelle Hardware, die wie eine Schutzmauer agiert: Durch unsichere Webseiten eindringende Schadsoftware bleibt in dieser Umgebung eingeschlossen und kann sich nicht auf dem Rechner und in dem lokalen Unternehmensnetzwerk verbreiten.

Die Virtualisierung trennt im ersten Schritt den Browser von dem restlichen PC. Für ein noch höheres Sicherheitsniveau können Unternehmen mit Browser in the Box das Internet vom internen Unternehmensnetzwerk, respektive dem Intranet, trennen. Mit dieser zusätzlichen Sicherheitskomponente wird mögliche Schadsoftware vom Netzwerk und der internen Infrastruktur ferngehalten. Diese weitere Isolation wird durch eine zusätzliche virtuelle Maschine mit gehärtetem Linux für den VPN-Client erreicht. Dieser baut einen VPN-Tunnel durch das Intranet (VPN-Protokoll: IPsec) zum Web-Gateway auf. Dieser leitet die Anfrage zum Internet dann im Klartext an das Internet weiter. Das gilt genauso für alle Daten, die vom Internet zurück zum Browser übertragen werden. Ein Angriff auf die Router und Switches des internen Netzwerks ist somit nicht mehr möglich, da alle Daten, die der Browser im Netzwerk erzeugt, in VPN-Pakete gekapselt/verschlüsselt werden, so dass ein Switch oder Router den Inhalt nicht interpretieren kann. Dadurch wird eine Trennung von Browser ↔Arbeitsplatz-PC und Intranet ↔Internet umgesetzt.

Da die Virtualisierungsschicht Kontrolle über die gesamte virtuelle Hardware hat, ist es möglich, den Zustand der virtuellen Maschine (Festplatte und Speicherinhalt) abzuspeichern und zu fixieren. Mittels dieses „Snapshot"-Mechanismus kann man einen sauberen Startzustand des Browsers fixieren. Falls der Browser während einer Internetsitzung durch Schadsoftware befallen wird, kann der Browser durch das Zurücksetzen auf den Startzustand gereinigt werden. Dies kann durch einen einfachen Neustart des Browsers umgesetzt werden. Das aufwendige Wiederherstellen eines PCs oder eines Terminal Servers wird durch einen einfachen Neustart des virtualisierten Browsers ersetzt.

Alle Arbeitsabläufe auf Windows laufen weiter wie gewohnt ab, Anwendungen wie Word und Excel werden wie gewohnt angewendet. Mit einem Klick auf das Browser in the Box-Icon auf ihrem Desktop startet der Webbrowser als eigenständige Instanz, es ist ein eigenständiger virtueller Rechner.

Abbildung 2: Isolation auf Netzwerkebene



4.2 Virtuelle/gemischte Infrastrukturen: Browser in the Box – Terminal Server

Für virtuelle Infrastrukturen mit Thin Clients oder Mischumgebungen mit Fat Clients und Thin Clients wurde Browser in the Box für Terminal Server entwickelt. In diesen Infrastrukturen läuft üblicherweise ein Windows Server in einer virtualisierten Umgebung, die durch Anbieter wie Citrix, VMware oder Microsoft bereitgestellt werden. Dieser Windows Server stellt jedem Benutzer eine Desktop-Sitzung bereit, welche auf dem Thin Client lediglich angezeigt wird.

In dieser Grundinstallation wird das Prinzip der Trennung von Intranet und Internet von Browser in the Box auch in dieser Produktvariante fortgeführt.

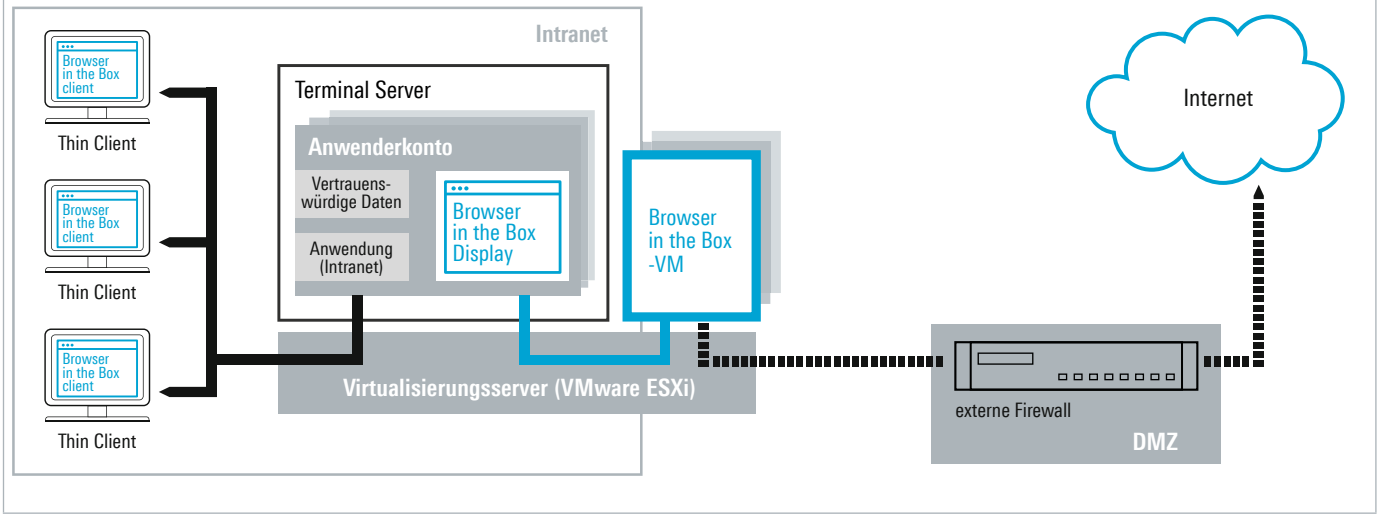
Anwendung von Browser in the Box – Terminal Server

Um Performance-Einbußen durch eine verschachtelte Virtualisierung zu vermeiden, wird diese Variante von Browser in the Box nicht innerhalb der Windows-Sitzung auf dem Terminal Server ausgeführt, sondern direkt auf der entsprechenden Virtualisierungsplattform als eigene, gekapselte Instanz. Lediglich die Anzeige des Browsers wird in die Desktop-Sitzung übertragen und dargestellt. Damit wird eine zuverlässige Trennung von Intranet Netzwerken und dem Internet ermöglicht. Diese flexible Architektur bindet Browser in the Box für Terminal Server in bestehende virtuelle Infrastrukturen ein.

Jeder Benutzer hat nach wie vor seine individuelle Browser in the Box-VM (VM = virtuelle Maschine). Die Trennung der Netzwerke wird durch VLANs umgesetzt, die in einer virtuellen Infrastruktur zur Verfügung stehen. Durch die VLANs wird der Internetverkehr der Browser in the Box-VM direkt in die DMZ und den Web Proxy geleitet. Internet und Intranet sind dadurch getrennt, ein VPN-Tunnel und das Browser in the Box-Web Gateway sind in diesem Szenario überflüssig.

Alle anderen Funktionen laufen genauso wie in der bisherig beschriebenen Version von Browser in the Box weiter. Dazu gehören die flankierenden Schutzmaßnahmen, wie das gehärtete Linux in der Browser in the Box-VM und das Zurücksetzen und Starten der Browser-VM bei jedem Start. Die administrativen Aufgaben, wie das Einrichten persistenter Konfigurationsdaten (Favoriten etc.) und die Rechtevergabe auf Nutzer- und Nutzergruppen-Ebene (Drucken, Uploads/Downloads etc.), bleiben selbstverständlich erhalten.

Abbildung 3: Das Funktionsprinzip von Browser in the Box – Terminal Server



4.3 Links in E-Mails, Word, pdfs – Die Browserweiche schafft Sicherheit

In Phishing-Mails werden oft Links zu schadhaften Webseiten untergebracht. Um das unerwünschte Herunterladen von Schadsoftware auf Webseiten[9] ebenfalls zu verhindern, wurde dafür eine sogenannte Browserweiche integriert: Ist der Link in der E-Mail nicht durch die unternehmenseigene Domain gekennzeichnet bzw. gehört die Domain nicht zu den von der IT-Administration spezifizierten Intranetseiten, dann öffnet sich automatisch Browser in the Box. Das gilt dann ebenfalls für Links in Word-Dokumenten, in PDFs und allen anderen Dokumentenarten.

Aber auch bei der Browserweiche kommt das Konzept der Netzwerktrennung (Intranet/Internet) zum Tragen: Mitarbeiter können im von der IT-Administration definierten Standardbrowser für Intranetanwendungen (z.B. das CRM-System im Internet Explorer) keine dem Internet zugehörigen Webseiten aufrufen. Denn der interne Browser ist ebenfalls vom Internet separiert. Das bedeutet, wenn im internen Browser z.B. ein Link auftaucht, der eigentlich zu einer nicht spezifizierten Domain gehört, dann öffnet sich die zum Link dazugehörige Webseite ebenfalls in Browser in the Box.

Die Browserweiche ist ein wichtiges Element in dem gesamten Sicherheitskonzept von Browser in the Box. Hiermit wird die Balance zwischen Sicherheit/Schutz vor Cyberangriffen und Usability und daraus resultierender Nutzerakzeptanz gehalten. Zum einen ist von Unternehmensseite die Sicherheit gewährleistet, weil in einem automatisierten Prozess die Netzwerktrennung auch während der Anwendung stattfindet. Auf der anderen Seite ist aus Nutzersicht der Aspekt der Usability sehr hoch, denn die Benutzung des Internets und Intranets kann wie gewohnt erfolgen.

4.4 Mobiler Einsatz von Browser in the Box

In einer mobilen Arbeitswelt ist selbstverständlich auch das sichere Internetsurfen unterwegs zu ermöglichen. Dafür gibt es auf Administrationsseite verschiedene Konfigurationsmöglichkeiten.

Zum einen kann man die mobile Nutzung („Mobile Use“) erlauben. Dann prüft der Browser in the Box-Client, ob er intern oder extern ist. Wenn er außerhalb des internen Unternehmensnetzwerkes aufgerufen wird, startet Browser in the Box, ohne dass ein VPN-Tunnel für den Zugriff auf das Internet aufgebaut wird.

Zusätzlich gibt es den „Hotspot-Modus“. Dieser ist für den Anwendungsfall bestimmt, wenn Mitarbeiter auch unterwegs immer über das Unternehmensnetzwerk und den VPN-Tunnel auch unterwegs auf das Internet zugreifen sollen. Sofern das Feature aktiviert wurde, wird beim Start von Browser in the Box zunächst überprüft, ob keine Internetverbindung besteht (durch pingen von vorher definierten IPs). Besteht keine Verbindung zum Internet, wird der Start von Browser in the Box fortgesetzt, um die Login-Seite des Internetanbieters am jeweiligen Hotspot aufzurufen. Nach Anmeldung am Hotspot muss der VPN-Client und durch die Eingabe der jeweiligen Zugangsdaten gestartet und Browser in the Box neu aufgerufen werden.

[9] Hier spricht man auch von Drive-by-Downloads

Zusammenfassung

Mit Browser in the Box von Rohde&Schwarz Cybersecurity ist die Annahme von vorneherein: Das Surfen im Internet birgt zu viele Gefahren. Um einen verlässlichen Schutz gegen Angriffe aus dem Netz zu bieten, ist der Ansatz bei Browser in the Box die Separierung kritischer Bereiche in voneinander isolierte Komponenten. Daraus ergeben sich folgende Vorteile für Unternehmen:

- **Proaktiver Schutz:**
  Trojaner, Viren, Ransomware, Advanced Persistent Threats und Zero-Day-Exploits haben durch die Zwei-Browser-Strategie keine Chance mehr. Internet und Intranet werden konsequent in voneinander isolierte Komponenten getrennt. Der Browser läuft auf einer eigenständigen virtuellen Maschine auf einem gehärteten Linux-Betriebssystem, der sich keinen Speicher mit dem Betriebs- und Dateisystem des Nutzers teilt. Durch die Anwendung von Virtualisierung ist selbst bei Infizierung des Browsers durch Schadsoftware nicht möglich, dass kritische Bereiche wie das Dateisystem des Nutzers oder die Infrastruktur des Unternehmens kompromittiert werden.

- **Einfache Implementierung und Administration:**
  Mit unserem Managementsystem namens TrustedObjects Manager (Hardware und Software) ist eine zentrale Verwaltung in der bestehenden IT-Architektur möglich. Dieser ist in der Lage, sich u.a. mit dem Windows-Verzeichnisdienst Active Directory und folglich ihren Nutzern im Netzwerk zu verbinden. Das ermöglicht den Rollout von Browser in the Box auf einzelne Mitarbeiter-PCs, aber auch auf ganze Nutzergruppen sowie eine Individuelle Rechtevergabe wie: Drucken, Uploads, Downloads oder Texte in Zwischenablage kopieren.

- **Trennung von Intranet und Internet auf Netzwerkebene:**
  Mit TrustedVPN, dem sicheren Web Gateway von Rohde&Schwarz Cybersecurity, werden Internet und Intranet nicht nur auf Rechnerebene, sondern auch auf Netzwerkebene voneinander isoliert.

- **Sicheres Surfen in Hotspots und im Homeoffice-WLAN:**
  Mit Browser in the Box und dem Hotspot-Modus in der Rechtevergabe ist der PC wirkungsvoll in öffentlichen WLANs, sogenannten Hotspots, vor Man-in-the-middle-Angriffen geschützt. Auch das sichere Surfen in privaten WLANs wie im Homeoffice ist möglich.

- **Einheitliche Durchsetzung von Compliance-Richtlinien:**
  Zur Absicherung des Unternehmensnetzwerkes wird oft jeglicher Traffic ins Internet durch eine Firewall oder/und einen Proxy-Server überprüft. Gleichzeitig gibt es mittlerweile schon Betriebsvereinbarungen, die Mitarbeitern das private Surfen im Internet erlauben. Diese Kombination ist aus Datenschutz- und Privatsphäregründen problematisch. Eine Filterung ist durch das Set-up von Browser in the Box aber nicht mehr nötig, denn hierüber kann jeglicher private Internetverkehr erfolgen.

- **Hoher Benutzerkomfort:**
  Aktive Inhalte werden unterstützt sowie Plug-Ins, Lesezeichen, Drucken und der Download oder Upload von Dateien. Die Browserkonfiguration (Lesezeichen, Plug-Ins, Proxy-Einstellungen etc.) wird im Benutzerkontext gespeichert → diese Daten werden beim Neustart nicht zurückgesetzt.

Produktvarianten:

- **Browser in the Box – Enterprise**
  Für den Einsatz auf Fat Clients und Workstations plus TrustedObjects Manager, der zentralen Managementappliance von Rohde&Schwarz Cybersecurity.

- **Browser in the Box – Terminal Server**
  Für den Einsatz auf Thin Clients mit zentralen virtuellen Infrastrukturen plus TrustedObjects Manager, der zentralen Managementappliance von Rohde&Schwarz Cybersecurity.

- **Browser in the Box – SMB**
  Für den Einsatz auf Fat Clients und Workstations in kleineren und mittleren Unternehmen.

Service mit Mehrwert

- Weltweit
- Lokal und persönlich
- Flexibel und maßgeschneidert
- Kompromisslose Qualität
- Langfristige Sicherheit

Rohde&Schwarz Cybersecurity
Das IT-Sicherheitsunternehmen Rohde&Schwarz Cybersecurity schützt Unternehmen und öffentliche Institutionen weltweit vor Spionage und Cyberangriffen. Mit über 500 Mitarbeitern entwickelt und produziert das Unternehmen technisch führende Lösungen für die Informations- und Netzwerksicherheit. Im Zentrum der Entwicklung vertrauenswürdiger IT-Lösungen steht der Ansatz „Security by Design“, durch den Cyberangriffe proaktiv verhindert werden.

Rohde&Schwarz
Der Elektronikkonzern Rohde&Schwarz bietet innovative Lösungen in folgenden Geschäftsfeldern: Messtechnik, Rundfunk- und Medientechnik, Sichere Kommunikation, Cybersicherheit sowie Monitoring and Network Testing. Vor mehr als 80 Jahren gegründet, ist das selbstständige Unternehmen mit seinem Firmensitz in München in über 70 Ländern mit einem engmaschigen Vertriebs- und Servicenetz vertreten.

Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

Rohde&Schwarz Cybersecurity GmbH
Mühldorfstraße 15 | 81671 München
Info: +49 30 65884-223
E-Mail: cybersecurity@rohde-schwarz.com
www.cybersecurity.rohde-schwarz.com

PD 5215.4475.61 | Version 01.01 | Oktober 2017 (sch)
Browser als Einfallstor für Cyberangriffe
Daten ohne Genauigkeitsangabe sind unverbindlich | Änderungen vorbehalten

5215447561

5215.4475.61 01.01 PDP 1 de