Wie Cyberangriffe über den Browser proaktiv verhindert werden können

Drei Szenarien, drei Lösungen

ROHDE&SCHWARZ
Cybersecurity

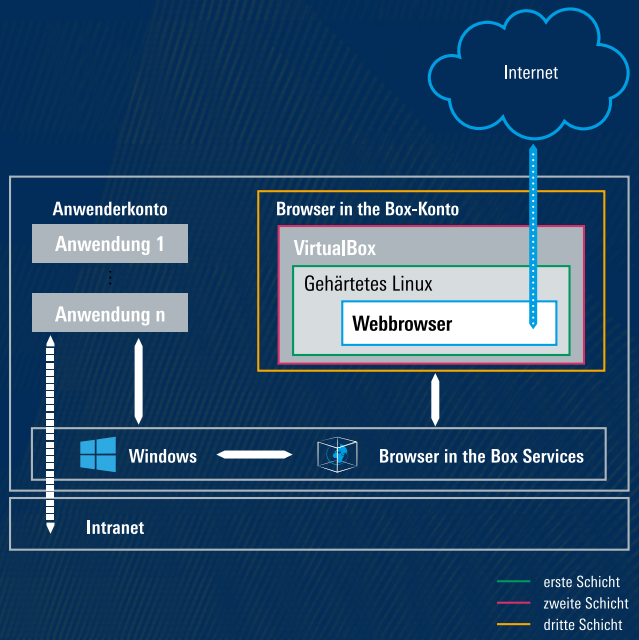
INHALTSVERZEICHNIS

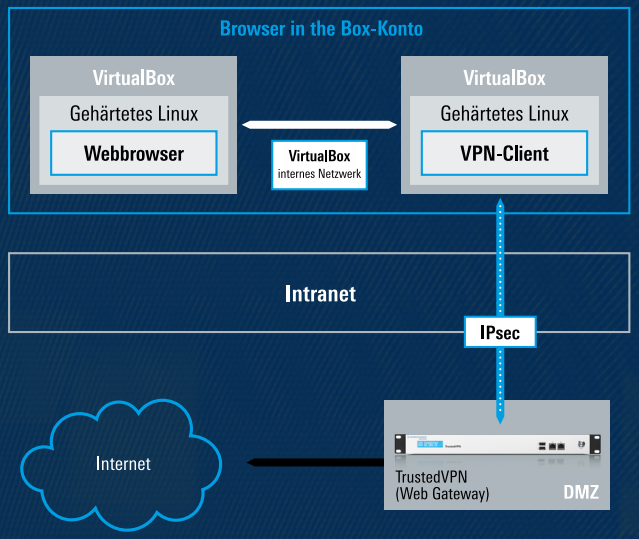
70% aller Cyberangriffe – wie Zero-Day-Exploits, Ransomware, Viren und Trojaner – erfolgen heute über einen Browser bzw. die besuchte Webseite. Problematisch sind dabei vor allem aktive Inhalte wie Flash, Java, JavaScript, ActiveX, aber auch HTML 5.

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. E-Mails mit schadhaften Links, die im Browser geöffnet werden und dann zu destruktivem Verhalten auf dem PC und im Netzwerk führen, sind die primäre Infektionsquelle. Danach kommen kompromittierte Webseiten.

Im Folgenden zeigen wir Ihnen konkret an drei Szenarien auf, wie Angriffe über den Internetbrowser erfolgen können. Und wie Sie mit der Lösung Browser in the Box von Rohde&Schwarz Cybersecurity das Einfallstor „Browser" für den Eintritt von Schadsoftware nachhaltig schließen. So surfen Ihre Mitarbeiter wie gewohnt im Internet und gleichzeitig sind PC und Unternehmensnetzwerk vor Angriffen geschützt.

DAS FUNKTIONSPRINZIP IN BILDERN





Der sicherste Browser der Welt:
Browser in the Box

Browser in the Box von Rohde&Schwarz Cybersecurity wurde ursprünglich im Auftrag des Bundesamts für Sicherheit in der Informationstechnik für den Einsatz in Bundesbehörden entwickelt. Der innovative Ansatz dabei ist, dass Betriebssystem und Browser vollständig voneinander getrennt sind.

Der Browser selber läuft auf dem PC in einer virtuellen Maschine, auf der ein speziell gehärtetes Linux als Betriebssystem eingesetzt wird. Im Gegensatz zu Sandboxing-Varianten wird hier der Speicher und Kernel nicht mit dem restlichen Windows-Betriebssystem geteilt. So ist auf Rechnerebene eine komplette Isolation möglich, Schadsoftware wird vom restlichen PC des Nutzers ferngehalten.

Zusätzlich wird auf Netzwerkebene der Zugang zum Internet vom Intranet getrennt. Das geschieht, indem sämtlicher Internetverkehr via VPN-Tunnel direkt zu einem Webgateway geleitet wird. Das interne Unternehmensnetzwerk (Intranet) ist somit komplett vom Internet getrennt. Für die Nutzer ändert sich nichts, sie surfen wie gewohnt im Internet. Und sollte man sich doch während einer Browsersitzung mit Schadsoftware infizieren, wird mit einem speziellen Mechanismus („Snapshot“) Browser in the Box nach Ende der Surfsession wieder auf seinen sauberen Ausgangszustand zurückgesetzt.

SICHERHEITSTIPP

E-Mails filtern:

⊕ Das automatisierte Filtern von E-Mail-Anhängen und -Typen, die potenziell gefährlich sind und nicht häufig verwendet oder für die tägliche Arbeit notwendig sind, ist eine Möglichkeit, das Risiko zu senken.

⊖ Locky oder andere Cyberangriffe der letzten Zeit zeigen: Hacker werden zunehmend besser, schadhaften Code in Dateitypen einzubinden, der mit E-Mail-Filtern nicht erkannt wird.

Schulung Mitarbeiter:

⊕ IT-Sicherheitsschulungen wären ein Weg, Mitarbeiter für das Erkennen von und Reagieren auf verdächtige E-Mails zu sensibilisieren.

⊖ Angriffe werden immer ausgefeilter und so ist es für Nutzer schwierig, Schadsoftware zu erkennen.

Schutz mit Browser in the Box

In Phase 2 wird der Link im Browser in the Box geladen. Da in dem Browser nur bestimmte Prozesse erlaubt sind, wird dieser unbekannte, gegebenenfalls nachgeladene Code nicht innerhalb der virtuellen Maschine des gehärteten Linux ausgeführt. Und kann sich daher nicht einmal in der virtuellen Maschine von Browser in the Box installieren. Darüber hinaus ist ein Ausbruch aus der virtuellen Maschine (kurz VM) nicht möglich und ein Angreifer wird niemals Zugriff auf die Unternehmensdaten erhalten können.

Szenario 1:
Phishing-Mail mit Trojaner

Phase 1

Der Nutzer erhält eine E-Mail, in der dieser auf einen Link klicken soll, um beispielsweise eine Information auf einer Webseite ansehen zu können. Der Absender ist augenscheinlich ein bekannter Kontakt. Der Nutzer klickt auf den Link in der E-Mail.

Phase 2

Der Link öffnet sich im Standardbrowser des Nutzers (meist Internet Explorer) und eine Seite wird geladen. Gegebenenfalls ist die Seite sogar so gut gemacht, dass dem Nutzern gar nicht auffällt, dass er sich bereits durch das einfache Öffnen der Seite einer Gefahr ausgesetzt hat. Phase 3 wurde bereits automatisch ausgeführt.

Phase 3

In dem Moment, wo die Seite bereits im Internet Explorer lädt, wurden auch Bildelemente und Skripte geladen, die so modifiziert wurden, dass hierdurch ein Angriff auf dem PC zur Ausführung kommt – beispielsweise ein modifiziertes JPEG-Bild, das auf der Seite eingebettet wurde, um einen Trojaner aus dem Internet nachzuladen.

Phase 4

Der nachgeladene Trojaner wird durch eine Schwachstelle auf dem System nachhaltig installiert. Meist geschieht dies tief in die Systeme hinein, um ein einfaches Entfernen verhindern zu können.

Phase 5

Direkt nach der Installation fängt der Trojaner an, zu seinem ursprünglichen Programmierer bzw. der zentralen Steuereinheit zurück zu kommunizieren. Der Angreifer weiß nun, dass er einen weiteren Computer auf der Welt übernommen hat und kann über den Trojaner alle Daten auf dem Computer UND im Unternehmensnetzwerk ausspähen, kopieren etc.

SICHERHEITSTIPP

Antivirussoftware/Firewall:

⊕ Bekannte Gefahren werden erkannt und die Ausführung der Schadsoftware wird gestoppt.

⊖ Hier kommt aber schon die Einschränkung: Bekannte Gefahren! Zero-Day-Exploits nehmen zu – Das sind Angriffe, die aufgrund von noch unbekannten Sicherheitslücken möglich sind. Deswegen ist die klassische Antivirussoftware/Firewall auch nur unzureichend. Dazu kommen gefälschte Entwicklerzertifikate, wodurch integrierte Sicherheitssysteme erst mal keinen Alarm schlagen.

Schutz mit Browser in the Box

1) Grundsätzlich ist durch die Netzwerktrennung, die bei Browser in the Box umgesetzt wird, für Word/Excel etc. der Internetzugriff nicht möglich, sodass die eigentliche Bedrohung nicht nachgeladen werden kann.

2) Browser in the Box wird aufgrund des geschützten Raums auch gerne als Dokumenten-Viewer benutzt. Darum kann man Dokumentenanhänge aus Mails am besten erst mal in Browser in the Box öffnen und sich den Inhalt anschauen. Mögliche Schadsoftware gelangt nicht auf den PC oder in das Unternehmensnetzwerk.

Szenario 2:
Mail mit Office-Dokument und schadhaftem Link

Phase 1

Ein vermeidlicher Geschäftskontakt schickt dem Mitarbeiter eines Unternehmens eine Excel-Tabelle mit Geschäftszahlen oder ein Word-Dokument mit einem Angebot. Der Mitarbeiter öffnet das Dokument, da er wissen möchte, was dieses Dokument beinhaltet.

Phase 2

Das Dokument öffnet sich in Word bzw. Excel. Es erscheint ein Hinweisfenster, das zum Anzeigen des Inhalts Makros aktiviert sein müssen. Der Mitarbeiter klickt auf den Knopf zum Aktivieren der Makros, sodass diese ausgeführt werden. Der Inhalt des Dokuments ändert sich jedoch nicht. Im Hintergrund läuft indes bereits Phase 3 unsichtbar für den Mitarbeiter ab.

Phase 3

Durch das Aktivieren der Makros in Word/Excel wird eine Folge von eingebetteten Anweisungen ausgeführt. Damit wird aus dem Internet eine Software nachgeladen, welche die Ransomware selbst beinhaltet.

Phase 4

Die Ransomware installiert sich im System und nutzt hierzu ggf. auch Privilege-Escalation*-Schwachstellen im System aus. Im Fall von bekannter Ransomware aus der Vergangenheit wurden Schwachstellen in Windows genutzt, um Zugriff auf das System zu gewinnen.

Phase 5

Nach der Installation kann die Ransomware mit seiner eigentlichen Aufgabe beginnen: Die Verschlüsselung von Unternehmensdaten auf dem System und im Unternehmensnetzwerk. Nach erfolgter Verschlüsselung wird eine Erpressernachricht angezeigt. Parallel hierzu verteilt sich meist die Ransomware auch noch lokal im Netzwerk weiter und nutzt hierzu weitere Schwachstellen in Microsoft Windows aus.

* Mehr Benutzerrechte in Windows erhalten, als eigentlich erlaubt wären

SICHERHEITSTIPP

Patch-Management/Aktuelle Software:

⊕ Exploit-Kits verlassen sich auf Softwareschwachstellen. Deswegen ist es wichtig, dass die eingesetzte Software gepatcht und aktuell ist.

⊖ Abhängig von der Größe und Komplexität Ihrer Organisation ist das Testen und Ausrollen der neuesten Patches ein Vollzeit-Job. Und: Bei unglaublichen 2 Milliarden langen Codezeilen z.B. bei Googles Produkten und einer durchschnittlichen Fehlerrate von 10 – 50 pro 1000 Zeilen ist klar, dass Sicherheitslücken in Software unvermeidlich sind.

Schutz mit Browser in the Box

Zum einen gilt hier: Schadcode wird vor allem fast ausschließlich gegen Windows-Systeme programmiert. Dieser Schadcode wird folglich in der Linux-VM nicht ausgeführt. Nur weniger als 1% des Schadcodes richtet sich an Linux-Betriebssysteme. Aber auch dann gilt: Alle Phasen laufen in der isolierten Umgebung von Browser in the Box ab. Die Schadsoftware verbleibt in der Virtual Machine und kann sich nicht auf dem restlichen PC ausbreiten. Mit der Snapshot-Methode wird nach Schließen und Neustart vom Browser in the Box der ursprüngliche, gereinigte Zustand des Browsers wiederhergestellt.

Szenario 3:
Exploit-Kits auf legitimen Websites

Phase 1

Ein Nutzer besucht eine legitime Webseite. In einem dort geschalteten Werbebanner hat ein Angreifer ein Exploit-Kit in Form eines schadhaften HTML-Tags eingeschleust. Der Code dieses Exploit-Kits ist dann darauf ausgelegt, nach Lücken im Browser oder in anderer Software zu suchen, wie z.B. dem Adobe Flash Player oder Microsoft Silverlight.

Phase 2

Die Erkennung des Schadcodes während des Angriffs wird durch Tarnung verhindert. In diesem Fall ist es ein iFrame, also der Werbebanner. Eine andere Methode ist, den bösartigen Code zu verschlüsseln, um die Erkennung zu verhindern.

Phase 3

Der Nutzer macht weiter nichts, klickt auf keinen Banner oder Link. Aber trotzdem scannt das Exploit-Kit, ob dieser Browser in einer veralteten Version mit einer bekannten Sicherheitslücke installiert ist.

Phase 4

Jetzt kann jede Form von Schadsoftware auf den PC des Nutzers heruntergeladen werden und den Rechner infizieren. Dieser Prozess wird als Drive-By-Download bezeichnet.

Phase 5

Im schlimmsten Fall infiziert diese Schadsoftware noch das Unternehmensnetzwerk, denn sie scannt alle verbundenen Laufwerke im lokalen Netzwerk und sucht dort einen Einstiegspunkt. Dann sind nicht nur der einzelne Rechner und seine Daten betroffen, sondern die Malware breitet sich auf das Intranet aus.

Fazit:
Sicher im Internet surfen mit Browser in the Box

Eine hundertprozentige Sicherheit kann es im Internet und im digitalen Zeitalter nicht geben. Zum einen sind Softwareprodukte durch ihre komplexen Codes immer anfällig für Sicherheitslücken. Auf der anderen Seite werden die Werkzeuge von Cyberkriminiellen immer ausgefeilter. Für Laien ist es schwer auszumachen, ob es sich jetzt z.B. um eine verdächtige Mail handelt. Aufgrund der Angriffsart des Social Engineerings, das ist der Angriff z.B. mit einer sehr authentischen Phishing-Mail an Mitarbeiter, sind IT-Sicherheitsschulungen in regelmäßigen Abständen unerlässlich.

Aber die Verantwortung kann nicht nur beim Nutzer liegen. Gleichzeitig müssen Systeme und Programme zum Einsatz kommen, welche Cyberangriffe im Vorfeld schon verhindern oder abmildern. Mit Browser in the Box brauchen Sie und Ihre Mitarbeiter sich keine Sorgen zu machen. Hier ist durch Isolation und Separierung sichergestellt, dass selbst bei einer Infizierung durch Schadcode nicht das gesamte System betroffen ist.

Erfahren Sie mehr unter:
www.cybersecurity.rohde-schwarz.com/browser-in-the-box

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

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

Version 01.00 | Oktober 2017 | Änderungen vorbehalten

Titelbild: ©istock.com – PeopleImages