Cyber-Sicherheit

Virtuell und sicher surfen

[20.03.2023] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt Behörden und Unternehmen zum Schutz vor Hackern erstmals einen Browser mit so genannten virtualisierten Instanzen. Clemens A. Schulz vom IT-Sicherheitsunternehmen Rohde & Schwarz Cybersecurity erklärt, wie ein solcher Browser funktioniert.

Herr Schulz, wie schätzen Sie die Bedrohungslage bei der Internet-Nutzung in Behörden und Unternehmen derzeit ein?

Als sehr hoch. Ransomware ist längst zum Massengeschäft krimineller Banden geworden. Jeden Tag fluten Zigtausende von Phishing-E-Mails die Postfächer von Mitarbeitenden. Sie sind optisch kaum mehr von echten E-Mails zu unterscheiden. Ein Klick auf den mitgesandten Link oder Anhang und die Malware hat freie Bahn zum gesamten Netzwerk. Bei vielen Angriffsmethoden muss der Nutzer nicht einmal mehr aktiv etwas anklicken, um sich mit einem Schad-Code zu infizieren.

Um Zugriff auf einen Rechner zu gelangen, genügt es Hackern also schon, wenn der Mitarbeitende nur im Internet surft?

Genau. Die Schad-Software wird bereits beim einfachen Laden der Web-Seite ausgeführt, ohne, dass der Nutzer Links anklicken oder Dateien öffnen muss. Aktive Inhalte wie JavaScript, Java oder Flash machen es möglich. Diese Programmierschnittstellen erlauben Hackern ohne Zutun des Nutzers den Zugriff auf den PC und die Kontrolle über dessen Anwenderumgebung. Traditionelle Sicherheitsmechanismen wie Antiviren-Software sind hier unwirksam. Neue Bedrohungen erfordern moderne, progressive Lösungen. Sehr wirksam ist eine Virtualisierung des Browsers.

Eine speziell abgesicherte, isolierte Browser-Umgebung mit virtualisierten Instanzen empfiehlt jetzt erstmals auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) für Behörden und Unternehmen mit besonderem Schutzbedarf. Was genau bedeutet das?

Eine Virtualisierung ist vergleichbar mit einer digitalen Quarantäne, in der die Malware eingeschlossen wird. Der Browser wird um eine virtuelle Surf-Umgebung ergänzt. Alle potenziell gefährlichen Aktivitäten werden in diesem geschlossenen virtuellen Browser isoliert, bevor sie überhaupt zur Ausführung kommen. Damit werden Attacken auf sensible Daten aus dem Internet erfolgreich abgewehrt, ohne dass der User in seiner Internet-Nutzung gehindert oder eingeschränkt wird. Zusätzlich wird auf der Netzwerkebene der Zugang zum Internet vom internen Unternehmens- oder Behördennetzwerk (Intranet) getrennt. Dieser Mechanismus schützt vor Angriffen via E-Mail-Anhängen, die Schad-Code erst im zweiten Schritt aus dem Internet laden, wie das bei der hochgefährlichen Schad-Software Emotet zum Beispiel der Fall ist, und macht gleichzeitig einen Datendiebstahl unmöglich. Zudem beseitigt jeder Browser-Start potenziellen Schad-Code und versetzt den Browser in seinen Ausgangszustand – was übrigens auch explizit vom BSI empfohlen wird.

„Betriebssystem und Browser haben zu keinem Zeitpunkt einen direkten Zugriff auf die Hardware, sondern lediglich auf die virtuelle Umgebung.“
Was macht die Vollvirtualisierung besser?

Bei einer Vollvirtualisierung wird sowohl vom Host-Betriebssystem des Clients als auch vom Intranet unabhängig gearbeitet. Betriebssystem und Browser haben auf diese Weise zu keinem Zeitpunkt einen direkten Zugriff auf die Hardware, sondern lediglich auf die virtuelle Umgebung. Eindringende Viren, Trojaner und Co. bleiben in dieser Umgebung eingeschlossen und können sich nicht auf dem Rechner und im lokalen Netzwerk verbreiten.

Und wie funktioniert das konkret?

Selbst wenn unabsichtlich Malware heruntergeladen wird, kann diese nicht in das interne Netz vordringen. Gleichzeitig kann die Schad-Software, wie zum Beispiel Ransomware oder Makroviren, keine Verbindung zum Internet herstellen, um die eigentliche Malware herunterzuladen. Ein großer Vorteil ist auch die Unabhängigkeit vom Betriebssystem. Indem auf das Host-System ein so genannter Hypervisor aufgesetzt wird, lässt sich ein vollwertiges eigenes Betriebssystem implementieren. Damit schafft man eine Systemdiversität, die es den Angreifern deutlich erschwert erfolgreich zu agieren.

Reicht ein solcher Browser als Schutz vor Angriffen aus?

Die Absicherung des Internets spielt eine zentrale Rolle – denn 70 Prozent der Hackerangriffe kommen aus dem Internet. Darüber hinaus sollten Unternehmen und Behörden aber auch weitere Schutzmaßnahmen vornehmen – beispielsweise die Verschlüsselung der Endgeräte, eine hochsichere VPN-Verbindung und die Absicherung des heimischen WLAN. Das IT-Grundschutz-Kompendium ist hier ein wichtiger Leitfaden für alle, die sich schützen wollen. Wir unterstützen unsere Kunden dabei, die jeweils passenden Lösungen zu finden.

Was bietet Rohde und Schwarz hierzu konkret an?

Der R&S Browser in the Box von Rohde & Schwarz Cybersecurity ist ein vollvirtualisierter Browser, der gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik für den Behördeneinsatz entwickelt wurde. Er sorgt für umfassende, mehrstufige Arbeitsplatzsicherheit.

()

Das BSI Grundschutz-Kompendium

Stichwörter: IT-Sicherheit, Cyber-Sicherheit, Rohde & Schwarz, Unternehmen