ROHDE&SCHWARZ
Make ideas real

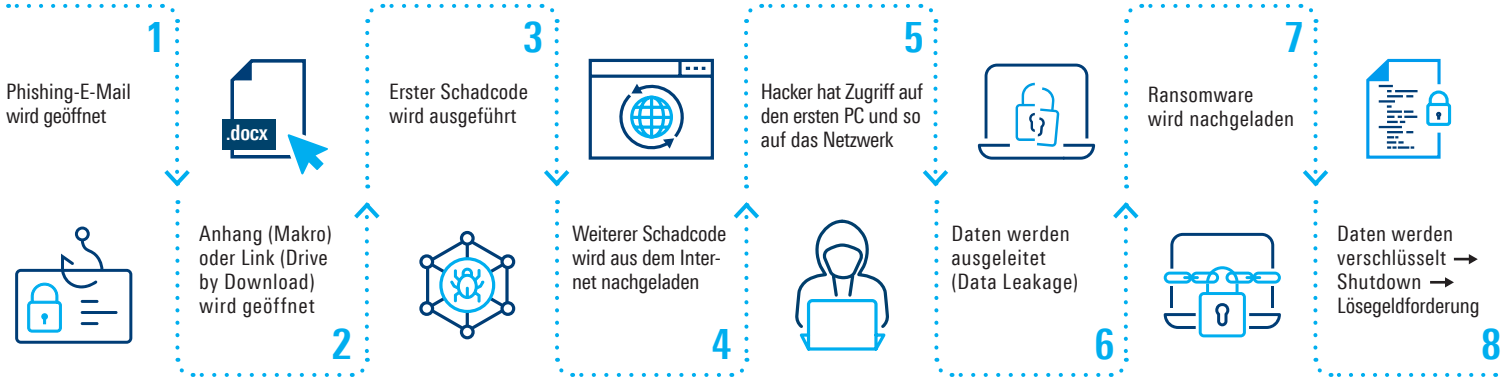
PROAKTIVER SCHUTZ VOR RANSOMWARE

WAS IST RANSOMWARE?

Die Zahl der Cyberangriffe nimmt stetig zu. Eine der häufigsten Angriffsarten ist der Einsatz von Malware: Schädliche Software, die in Netzwerke eindringt. Malware hat sich mittlerweile zu einer Art Werkzeugkasten für Cyberkriminelle entwickelt. Das meistverwendete Malware-Werkzeug ist dabei Ransomware – Schadprogramme, die den Zugriff auf Daten und Netzwerke einschränken oder verhindern, Daten ausleiten können und diese Ressourcen nur gegen Zahlung eines Lösegeldes wieder freigeben. Dabei verschlüsselt die Schadsoftware Dateien oder den ganzen Computer.

Ransomware hat eine Entwicklung vom gefälschten Antivirus-Produkt zur Malware mit fortschrittlichen Verschlüsselungsfunktionen durchgemacht, mit der **Unternehmen**, immer mehr aber gezielt **KRITIS** und der **öffentliche Sektor** angegriffen werden. Die Verbreitung erfolgt häufig über **Phishing**-E-Mails, versteckt in Bildern oder als ausführbare Dateien im Anhang von E-Mails.

WIE LAUFEN RANSOMWARE-ANGRIFFE IN DER REGEL AB?



Die per Makro (z. B. aus einem Microsoft Office-Dokument) oder Phishing-Link geladenen Einstiegspunkte sind lediglich eine Art Basis-Malware. Ihre Hauptaufgabe besteht darin, im Idealfall bei jedem Angriff etwas anders auszusehen, um von den klassischen Antiviren-Scannern nicht erkannt zu werden. Die eigentliche Bedrohung wird über einen verschlüsselten Kanal innerhalb des Malware-Loaders nachgeladen: Programme, die Daten und Passwörter ausleiten und im Anschluss die ausgespähten Daten verschlüsseln.

WIE HAT SICH RANSOMWARE ENTWICKELT?

Neben dem enormen Schadenspotenzial gewinnt Ransomware auch durch konstant steigende Fallzahlen an Relevanz im Bereich Cybercrime. Im internationalen Vergleich ist Deutschland überdurchschnittlich häufig von Ransomware-Angriffen betroffen. Das **Bedrohungspotenzial** ist im Jahr 2021 nochmals deutlich angestiegen. Laut Bundeskriminalamt ist Ransomware zudem die Vorgehensweise mit dem höchsten Schadenspotenzial im Bereich Cybercrime. Der **Branchenverband Bitkom** ermittelte beispielsweise seit 2019 bis Ende 2021 einen Anstieg der Schäden um 358 Prozent. Und es ist damit zu rechnen, dass dieser Trend in Zukunft weiter zunimmt.

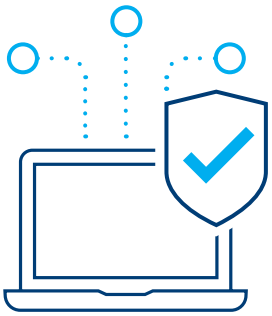
Während die Angreifer vor einiger Zeit noch einzelne Computer verschlüsselten und Lösegeld pro verschlüsseltem PC verlangten, spionieren sie heute betroffene Behörden- oder Unternehmensnetzwerke zunächst gezielt aus. Dabei werden oftmals Daten ausgeleitet (**Data Leakage**) und eine Bewertung des jeweiligen Opfers vorgenommen. Die Täter passen ihre Lösegeldforderung dann der betroffenen Organisation an. Die sogenannte **Double Extortion** hat sich inzwischen als Standard bei Ransomware-Angriffen etabliert. Hierbei erfolgt die Erpressung durch Verschlüsselung der Systeme bei gleichzeitiger Drohung mit Veröffentlichung abgeflossener, sensibler Daten. In diesem Fall hilft auch eine gute Backup-Strategie nicht mehr.

Ein weiterer alarmierender Trend ist **Ransomware as a Service** (**RaaS**): Cyberkriminelle müssen heute nicht mehr zwangsläufig über die technischen Fähigkeiten zur Programmierung von Schadsoftware verfügen, sondern können auf ein umfangreiches Angebot an Schadsoftware gegen Bezahlung zurückgreifen. So ist es für Angreifer immer einfacher, auch komplexere Angriffe auszuführen.

WARUM IST ES WICHTIG, JETZT ZU HANDELN?

- Hacker gehen immer ausgeklügelter vor und fordern höhere Lösegelder.
- Die Kosten für Ausfallzeiten werden oft unterschätzt.
- Data Leakage hat den Verlust von Reputation zur Folge – und dadurch entsteht für die betroffenen Unternehmen ein immenser Schaden.
- Eine Backup-Strategie alleine reicht nicht mehr als Absicherung aus.
- Auch bei Zahlung der Lösegeldforderungen gibt es keine Garantie dafür, dass die Hacker keinen Systemzugriff mehr haben oder die gestohlenen Daten auch tatsächlich löschen oder wieder freigeben.

WAS KÖNNEN SIE TUN?



1. Spielen Sie Sicherheitspatches regelmäßig und zeitnah auf und führen Sie regelmäßig Sicherheitsupdates aus.
2. Der Gerätelebenszyklus ist ein wichtiger Bestandteil der Netzwerksicherheit. Veraltete Systeme mit nicht mehr unterstützten Betriebssystemen wie Windows XP sollten unter keinen Umständen in einem mit dem Internet verbundenen Netzwerk laufen.
3. Öffnen Sie keine E-Mail-Anhänge oder Links, die nicht zweifelsfrei sicherer Herkunft sind.
4. Laden Sie nur Programme aus dem Internet, die von verifizierten Stellen angeboten werden.
5. Erstellen Sie regelmäßig Backups auf externen Datenträgern.

Fast alle Unternehmen und Behörden verfügen über grundlegende Schutzmaßnahmen. Doch diese reichen nicht aus, um sich gegen hochspezialisierte Cyber-Angriffsmethoden abzusichern. **Wer sich umfassend und proaktiv vor Ransomware-Angriffen schützen will, muss noch einen Schritt weitergehen.**

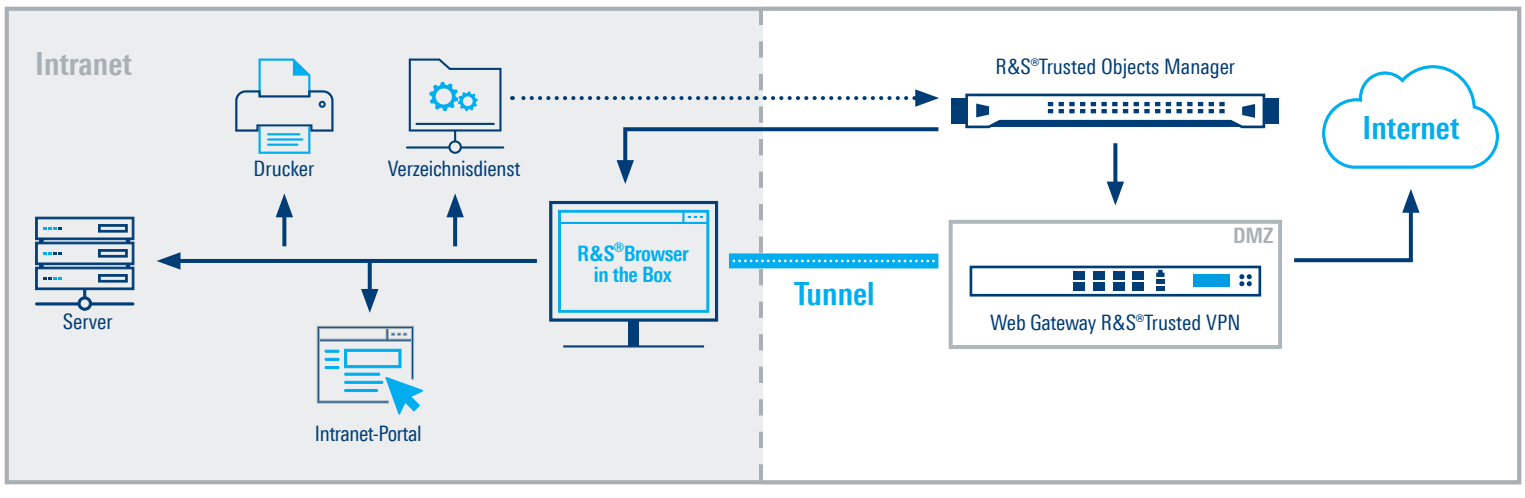
WIE SCHÜTZEN SIE SICH PROAKTIV?

Die Internetnutzung ist aus dem beruflichen Alltag nicht mehr wegzudenken. Aber der dafür benötigte Browser dient als Einfallstor für Ransomware und andere weit verbreitete Schadsoftware.

Die zusammen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte **vollvirtualisierte Surfumgebung** R&S®Browser in the Box bietet ein innovatives, mehrstufiges Konzept für sicheres und komfortables Surfen im Internet und optimalen Schutz vor Schadsoftware für Behörden und Unternehmen. R&S®Browser in the Box hat dabei zwei Schutzziele: Die Isolation auf Rechnerebene und die Isolation auf Netzwerkebene.

Bei der **Isolation auf Rechnerebene** schließt der virtuelle Browser die Sicherheitslücke „Internet“, indem er eine digitale Quarantäne für Angriffe ermöglicht: Schadsoftware wird isoliert, bevor sie überhaupt zur Ausführung kommt. Anstatt – wie bei Antivirenprogrammen – Schadcodes zu erkennen, wird von vorneherein die Ausführung verhindert. Alle potenziell gefährlichen Aktivitäten werden in einem geschlossenen virtuellen Browser isoliert. Dabei werden Betriebssystem und Browser komplett voneinander getrennt. So lassen sich z.B. auch Malvertising-Angriffe verhindern, bei denen sich in vermeintlich seriösen Banner-Anzeigen Schadcodes verbergen. Diese werden beim Anklicken der Anzeige auf den Rechner heruntergeladen. Die Malware deaktiviert dann verschiedene Sicherheitsmechanismen und kann sich effizient auf dem System und dem Netzwerk ausbreiten. Anschließend werden per Ransomware persönliche und geschäftliche Daten verschlüsselt und so unzugänglich gemacht.

In Bezug auf Ransomware-Angriffe (und Malware-Angriffe allgemein) entscheidend ist jedoch das zweite Schutzziel – die **Isolation auf Netzwerkebene.** Durch den komplett uneingeschränkten Internetzugang im gekapselten Browser benötigt das eigentliche Endnutzer-Betriebssystem nur noch Zugang zu sehr selektiv ausgewählten Webservern. Der Internetzugriff kann dadurch deutlich feingranularer gesteuert werden und so ist es möglich, den Zugang ausschließlich auf vertrauenswürdige Server im Internet zu beschränken. Das schließt alle Server und Dienste im Internet aus, die von Hackern bereitgestellt werden. Und wenn der Zugriff auf die Server der Hacker nicht möglich ist, kann Malware keinen Schaden am Computersystem verursachen – der Angriff wird damit unterbunden.



Vorteile von R&S®Browser in the Box:

- Sicherheit durch **Vollvirtualisierung und Trennung von Internet und Intranet**
  - Optimaler Schutz vor Schadsoftware durch Blockierung von Malware-Nachladung
  - Verhinderung von Data Leakage
  - Proaktive Blockierung aller Telemetriedienste
- **Zwei-Browser-Strategie**
  - Intranetbrowser für Intranetportale
  - R&S®Browser in the Box für Internet (Firefox, Chrome, Tor-Browser für Spezial-Anwendungsfälle)
- Für **Arbeitsplatz-PCs** und **Terminalserver-Umgebungen**
- In Kooperation **mit dem BSI** entwickelt

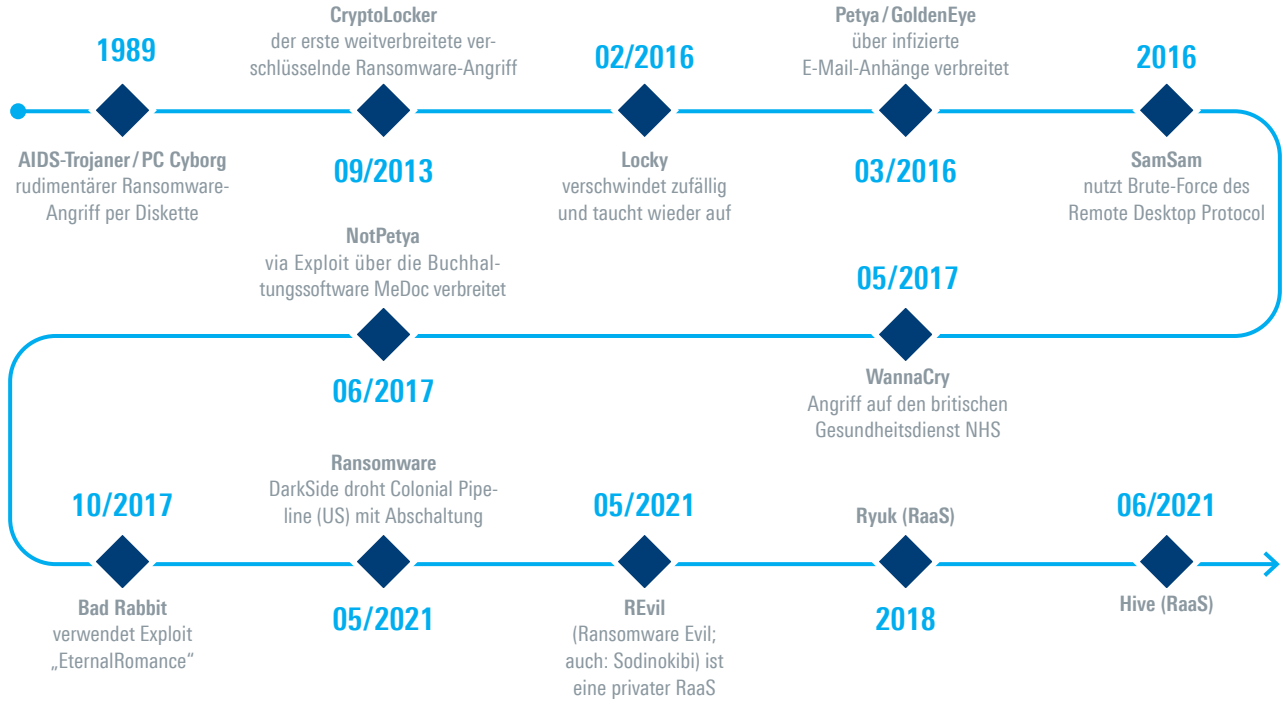
Häufige Fragen zu R&S®Browser in the Box

Wie verhindert R&S®Browser in the Box Schadsoftware-Angriffe (wie zum Beispiel Emotet)?
Malware-Angriffe werden heutzutage vor allem über Command & Control Server gesteuert: Der Malware-Loader kommuniziert mit den Servern und lädt die entsprechenden Programme nach Anweisungen nach. Durch den Einsatz von R&S®Browser in the Box wird diese Kommunikation vollständig unterbunden. Somit ermöglicht es die Lösung, zum Beispiel Emotet gänzlich auszuschalten, da ohne Kommunikation keine Anweisungen ausgeführt werden können.

Ersetzt R&S®Browser in the Box Virenscanner / Firewalls?
Nein. Unsere Lösung wird zusätzlich zu den Basis-Schutzmaßnahmen wie zum Beispiel Firewalls oder Virenscanner eingesetzt. Erst durch die so mögliche Trennung von Intranet und Internet können sich Unternehmen und Organisationen wirksam vor Cyberangriffen schützen.

Gibt es Einschränkungen bei der Internetnutzung?
Unsere Lösung selbst schränkt die Internetnutzung nicht ein. Administratoren können jedoch Einschränkungen festlegen, z. B. welche Dateitypen heruntergeladen werden dürfen oder ein komplettes Upload-Verbot.

Sind Videochats/Videokonferenzen möglich?
Ja. Videochats und -konferenzen sind beim Einsatz von R&S®Browser in the Box problemlos in allen etablierten Videokonferenzlösungen möglich.



Rohde & Schwarz Cybersecurity GmbH
Mühldorfstraße 15 | 81671 München
Info: +49 30 65884-222
E-Mail: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

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

PD 3683.3842.31 | Version 02.00 | Dezember 2022 (NP)

3683384231

3683.3842.31 02.00 PDP 1 de