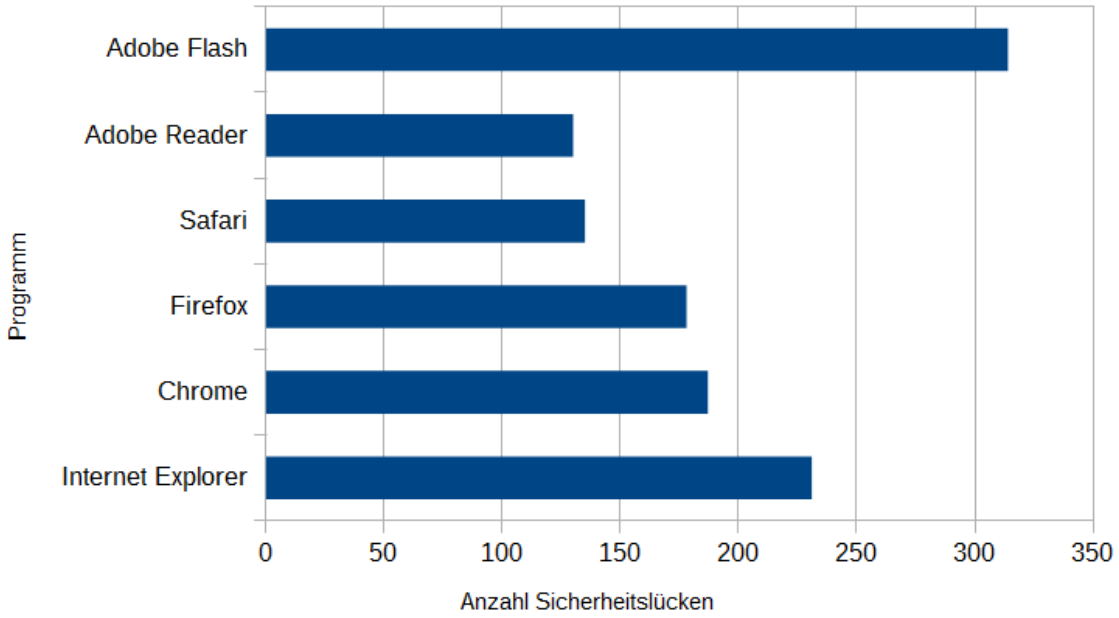
Die Ausgangssituation

Trotz konventioneller Abwehrmaßnahmen kann nicht verhindert werden, dass Malware und Schadcode über USB-Sticks, E-Mail-Anhänge und das Surfen im Internet in ein Unternehmensnetz eindringen. Vor allem Sicherheitslücken im Internetbrowser sind ein zentraler Angriffspunkt für zahlreiche Schadprogramme. Auch die weit verbreiteten Adobe-Applikationen erweisen sich immer wieder als gefahrenträchtig.



Selbst bei einem fortgeschrittenen Firewall-Konzept mit Demilitarisierter Zone (DMZ) kann der Browser zum Einfallstor in das Unternehmensnetz werden. Gelangt ausführbarer Schadcode durch eine Sicherheitslücke im Webbrowser in das interne Netz, so wird er mit den Systemberechtigungen des angemeldeten Benutzers ausgeführt. Angreifer erhalten so Zugriff auf dieselben Systeme, Daten und Anwendungen, die auch dem angemeldeten Benutzer zugänglich sind. **Es drohen Systemausfall, Manipulation, Sabotage und Wirtschaftsspionage.**

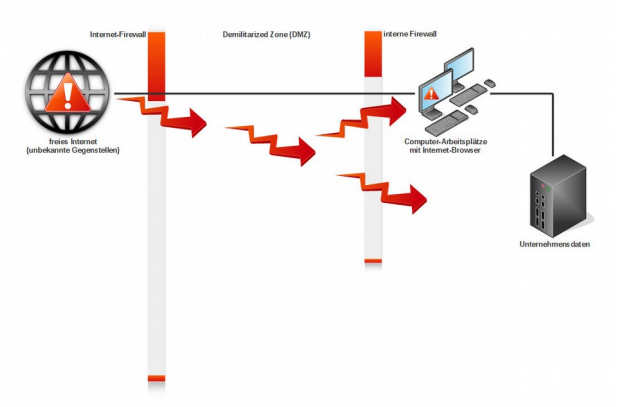


Abbildung 1: Angriff aus dem Internet

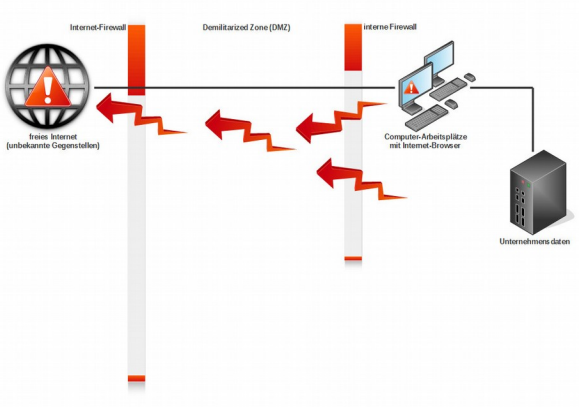


Abbildung 2: Datenabfluss in das Internet

In klassischen Installationen wird der Browser im internen Netzwerk ausgeführt. Potenziell bösartige Webinhalte aus dem offenen Internet werden folglich dort interpretiert, wo sie vielfältigen Schaden anrichten können. Dabei spielt es keine Rolle, ob der Browser auf Arbeitsplatzcomputern, auf Terminalservern oder in speziellen Sandbox-Umgebungen ausgeführt wird. In allen Fällen ist die Trennung von der internen IT-Umgebung nur schwach. Insbesondere Datendiebstahl ist in diesem Zusammenhang eine ernst zu nehmende Bedrohung. Ist Schadcode einmal ins interne Unternehmensnetz gelangt, kann er Unternehmensdaten über die Schnittstelle des Browsers ins Internet abfließen lassen – und das oft über einen langen Zeitraum unbemerkt.

Die technisch machbare, vollständige Trennung interner Netzwerke vom Internet kommt aus betrieblichen Gründen kaum noch infrage. Internetrecherchen gehören zum Unternehmensalltag, zentrale Prozesse von Produktion, Verwaltung und Kommunikation werden routinemäßig über das Internet abgewickelt. Internetangebote und Multimedia-Anwendungen müssen daher unter Berücksichtigung aller Sicherheitsanforderungen jederzeit verfügbar bleiben.

Konventionelle Maßnahmen wie das Filtern von URL-Adressen oder das Blocken bestimmter Inhalte erhöhen die Sicherheit allenfalls temporär. Sie bringen jedoch hohen Administrationsaufwand mit sich und schränken AnwenderInnenen mehr oder minder stark ein. Vor allem arbeiten sie rein symptomatisch und bekämpfen nicht die Ursache des Problems. So werden etwa auch seriöse Websites ohne Wissen der Betreiber immer wieder Opfer einer Kompromittierung und gefährden als „Malware-Schleudern“ die IT-Sicherheit ahnungsloser BenutzerInnen.

Abwehrmaßnahmen wie Intrusion Detection Systems (IDS) oder Virenscanner schützen nur begrenzt, da sie auf bekannte Angriffsmuster spezialisiert sind. Weltweit gelangen jedoch täglich neue Schadcodes und Angriffsstrategien in den Umlauf: ein letztlich aussichtsloses Katz-und-Maus-Spiel im Hinblick auf reaktive Schutzsysteme.

Die Lösung

Der ideale Webbrowser hat zwar Internetzugang, soll aber auf interne Daten und Ressourcen nicht zugreifen. Er darf folglich nicht im internen Netz ausgeführt werden, muss jedoch zugleich vom Arbeitsplatz aus steuerbar und sichtbar sein. Diese auf den ersten Blick unvereinbaren Anforderungen werden mit dem Remote-Controlled Browser-System (ReCoBS) **TightGate-Pro** sicherheitstechnisch einwandfrei und aus Anwendersicht komfortabel umgesetzt.

Bei **TightGate-Pro** wird der Browser nicht im internen Netzwerk, sondern innerhalb der DMZ auf dem dedizierten ReCoBS-Server ausgeführt. Der für den Anwender relevante Bildschirminhalt wird in Form von Bild- und Tondatenströmen verschlüsselt an die Arbeitsplatzrechner übertragen. Umgekehrt ist eine Fernsteuerung des Browsers vom Arbeitsplatz aus möglich. **Das Internet kann vollfunktional genutzt werden.**

Das entscheidende Sicherheits-Plus: Jetzt kann das interne Netzwerk über geeignete Firewall-Regeln **vollständig** gegenüber dem offenen Internet abgeschottet werden. Es ist damit für Angreifer aus dem Internet prinzipiell unerreichbar. In der Gegenrichtung wird ungewollter Datenabfluss zuverlässig unterbunden. **Das Schutzniveau des internen Netzwerks bleibt jederzeit maximal.**

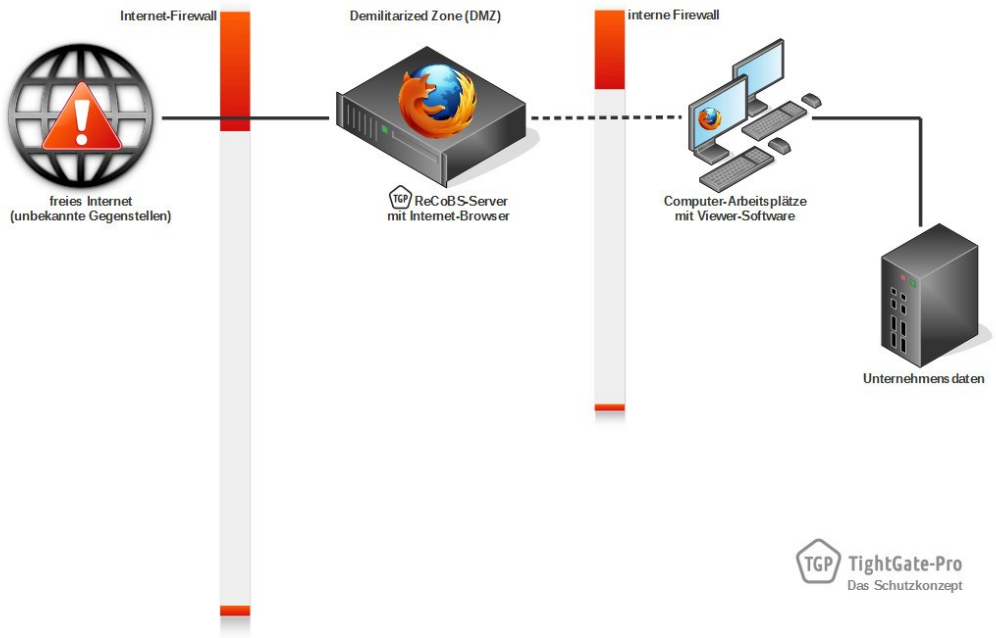


Abbildung 3: TightGate-Pro trennt das interne Netzwerk vom Internet.

TightGate-Pro implementiert eine benutzerfreundliche **Zwei-Browser-Lösung**:

1. Das offene **Internet** steht über **TightGate-Pro** risikofrei zur Verfügung.
2. Ein **Intranet** ist über einen lokal installierten Browser zugänglich.

Der nur zum internen Gebrauch vorgesehene, lokale Browser kann einen beliebigen Softwareversionsstand aufweisen oder mit speziellen Erweiterungen ausgestattet sein. Da er nicht über Internetzugang verfügt, ist eine Gefährdung des internen Netzwerks ausgeschlossen. Unternehmensspezifische Fachanwendungen über vertrauenswürdige Gegenstellen können anhand einer Whitelist in der Internet-Firewall freigeschaltet werden.

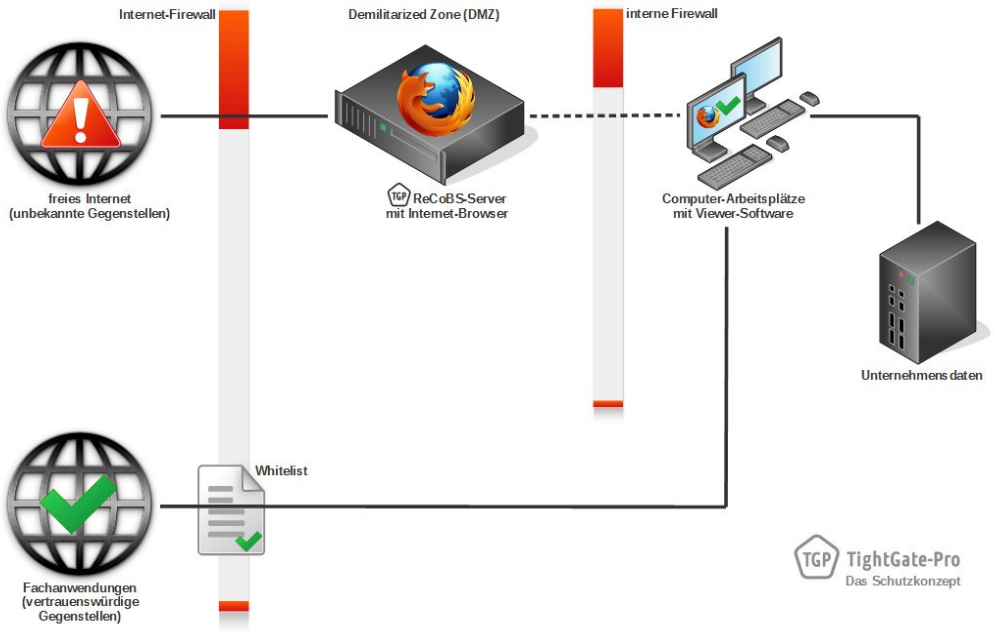


Abbildung 4: Intranet und Fachanwendungen bleiben wie gewohnt nutzbar.

Mobile Rechner unterwegs oder im Homeoffice sind nicht weniger schutzbedürftig als stationäre Arbeitsplatzplatzrechner – im Gegenteil. Allerdings ist deren Netzwerkanbindung beispielsweise über WLAN oder UMTS mit geringerem Datendurchsatz ausgestattet. Eine Nutzung des Internets über **TightGate-Pro** wird hierdurch erschwert.

TightGate-Mobile stellt eine virtuelle Umgebung bereit, die den gefährdeten Internetbrowser auf Mobilrechnern isoliert. Mit **TightGate-Mobile** ist sichere Internetnutzung auf Reisen, bei Geschäftspartnern oder im Homeoffice kein Problem. Die optimale Lösung auch für stationäre PCs außerhalb des Firmennetzwerks.

Das TightGate-Prinzip

Während der Internetbrowser bei **TightGate-Pro** auf dem ReCoBS-Server ausgeführt wird, erfolgt die Anzeige der Bildschirmausgabe auf dem Monitor des Arbeitsplatzcomputers. Zugleich kann der Browser auf dem ReCoBS-Server vom Arbeitsplatz aus ferngesteuert werden.

Aufgrund dieser physischen Trennung bleibt selbst der Aufruf einer kompromittierten Internetseite für das interne Netzwerk folgenlos. Durch Drive-by-Downloads oder Links von Phishing-E-Mails (Link-Spoofing) kann kein Schaden entstehen. Interne Unternehmensdaten bleiben vor Angriffen aus dem Internet geschützt.

Auch wenn NutzerInnen versehentlich Anhänge öffnen, potenziell gefahrenträchtige Seiten aufrufen oder fragwürdigen Links folgen, ist das interne Netzwerk für Angreifer aus dem Internet unerreichbar. Zugleich können Unternehmensdaten nicht ungewollt ins Internet abfließen.

Mit **TightGate-Pro** ist Internetnutzung komfortabel möglich.
Angriffe aus dem Internet, Ausspähung und Wirtschaftsspionage werden verhindert.

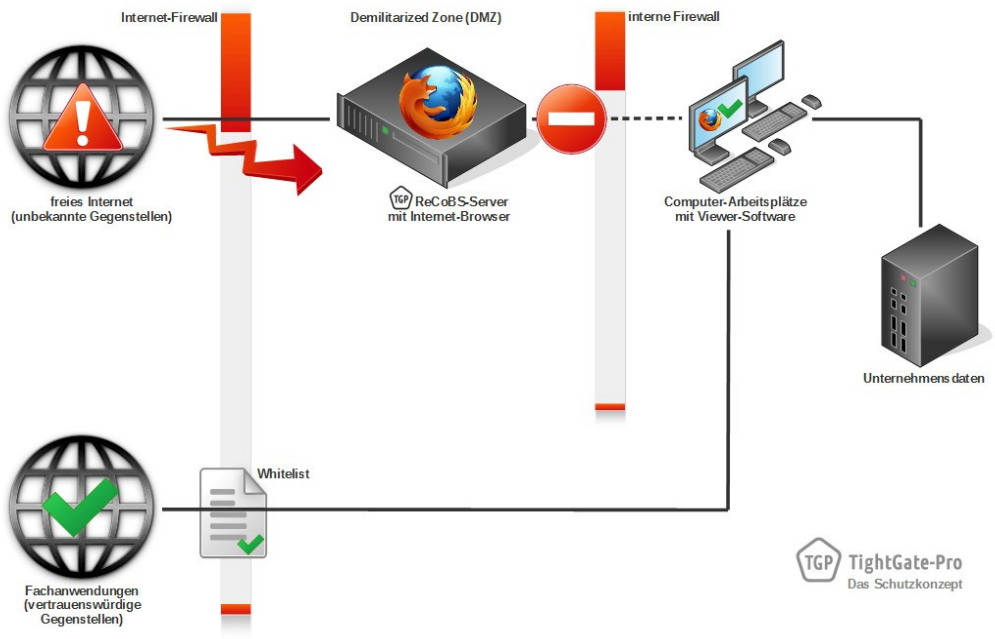


Abbildung 5: Angriffe aus dem Internet werden verhindert, Datenabfluss ebenfalls.

TightGate-Pro macht die Internetnutzung sicher und schützt zugleich vor unbeabsichtigtem Datenabfluss – selbst wenn über **andere Wege** Schadcode ins interne Netzwerk gelangen sollte. Auch USB-Sticks oder E-Mail-Anhänge können bösartigen Code enthalten. Da das interne Netzwerk durch **TightGate-Pro** vom Internet abgeschottet ist, kann Schadsoftware weder weiteren Code aus dem Internet nachladen noch interne Daten versenden.

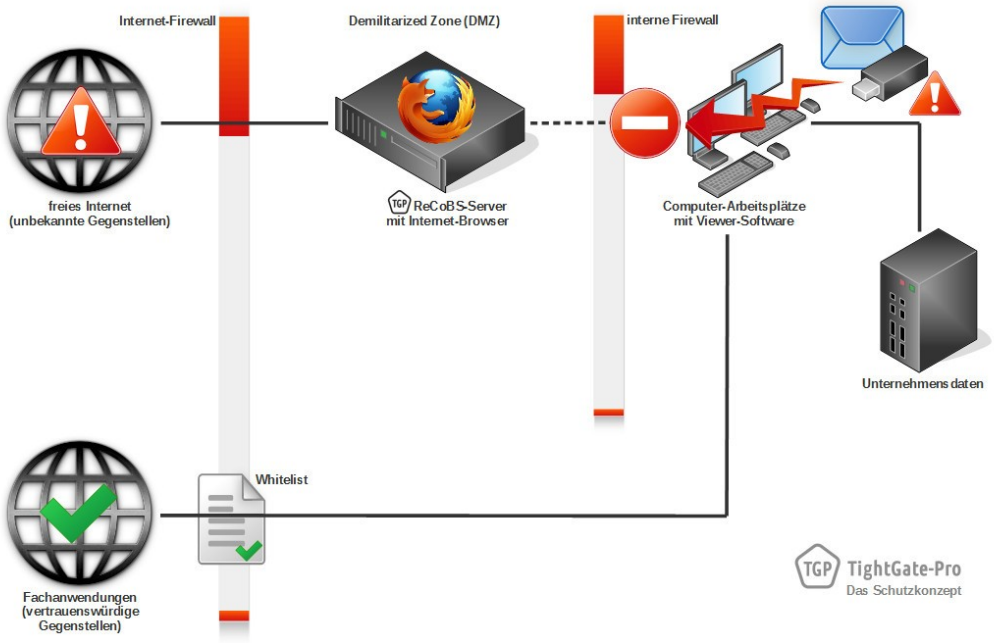


Abbildung 6: Auch Schadcode aus anderen Quellen wird isoliert.

Eine umfangreiche Härtung des ReCoBS-Servers macht **TightGate-Pro** zu einem zweistufigen Schutzsystem. Eine Kompromittierung des ReCoBS-Servers (erste Schutzstufe) durch Angriffe über den Internetbrowser ist aufgrund weitreichender Maßnahmen auf Betriebssystemebene sehr unwahrscheinlich. Zusätzlich ist die physische Trennung des internen Netzwerks vom Internet infolge des VNC-ähnlichen, funktionsspezifischen Protokolls (zweite Schutzstufe) für potenzielle Angreifer nahezu unüberwindbar.

Mit **TightGate-Pro** wird die gefahrlose und komfortable Nutzung des Internets Realität – bei zugleich umfassender Kontrolle im Hinblick auf die vollständige Abschirmung des internen Netzwerks.