nrw-unITS
IT-Sicherheit
Nordrhein-Westfalen

Surfen im Büro? Aber sicher!

03.04.2014

Dr. Norbert Schirmer
Sirrix AG

Sirrix AG
security technologies

Ministerium für Wirtschaft, Energie, Industrie, Mittelstand und Handwerk des Landes Nordrhein-Westfalen

EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds
für regionale Entwicklung

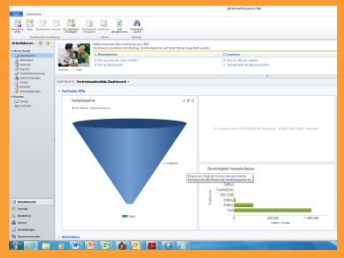
Web-Browser heute unverzichtbar

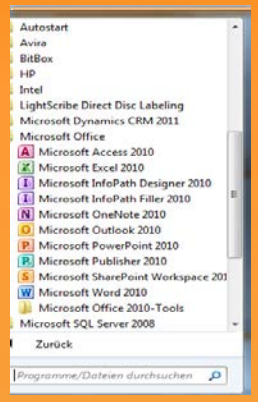
nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

Arbeitsplatzrechner

INTRANET

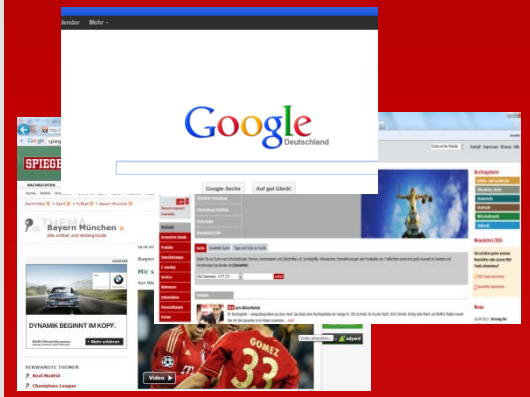
- Produktbezogene Daten
- Produktentwicklungsunterlagen
- Strategische Konzepte
- Emails





INTERNET

- Recherchen
- Nachrichten



Sirrix AG
security technologies

Gefahrenschwerpunkt Webbrowser

nrw-units IT-Sicherheit Nordrhein-Westfalen

- Das größte Einfallstor für Gefährdungen aus dem Internet ist der Web-Browser

Sicherheitslücke

Bundesamt warnt vor Nutzung von Internet Explorer

Internet Explorer: Bundesbehörde warnt vor Sicherheitslücke

Betroffen sind Nutzer von Windows XP und Windows 7: Drei Versionen de Microsoft-Browsers Internet Explorer weisen gravierende Sicherheitslücken auf, die für Angriffe genutzt werden. Bis zur Lösung des Problems bietet Microsoft einen vorläufigen Schutz zum Download an.

heise Security

News | Hintergrund | Erste Hilfe

Security > News > 7-Tage-News > 2012 > KW 36 > Java-Sandbox auch in aktueller Version angreifbar

03.09.2012 07:41 « Vorige | Nächste »

Java-Sandbox auch in aktueller Version angreifbar

vorlesen / MP3-Download

Das am Donnerstag vergangener Woche veröffentlichte Java 7 Update 7 stoppt zwar alle öffentlich bekannten Exploits, ist laut dem polnischen Sicherheitsforscher Adam Gowdiak jedoch weiterhin verwundbar. Auf der Sicherheits-Mailingliste Bugtraq berichtet Gowdiak, dass er in der aktuellen Java-Version eine Sicherheitslücke gefunden hat, die sich in Kombination mit bereits zuvor von ihm entdeckten Lücken wieder zum Abschalten der Sandbox eignet. Ein Angreifer könnte dies Ausnutzen, um Besucher einer speziell präparierten Webseite mit Schadcode zu infizieren.

→ Web-Browser Sicherheit muss im Fokus aller Endpoint-Security Anstrengungen stehen

Sirrix AG security technologies

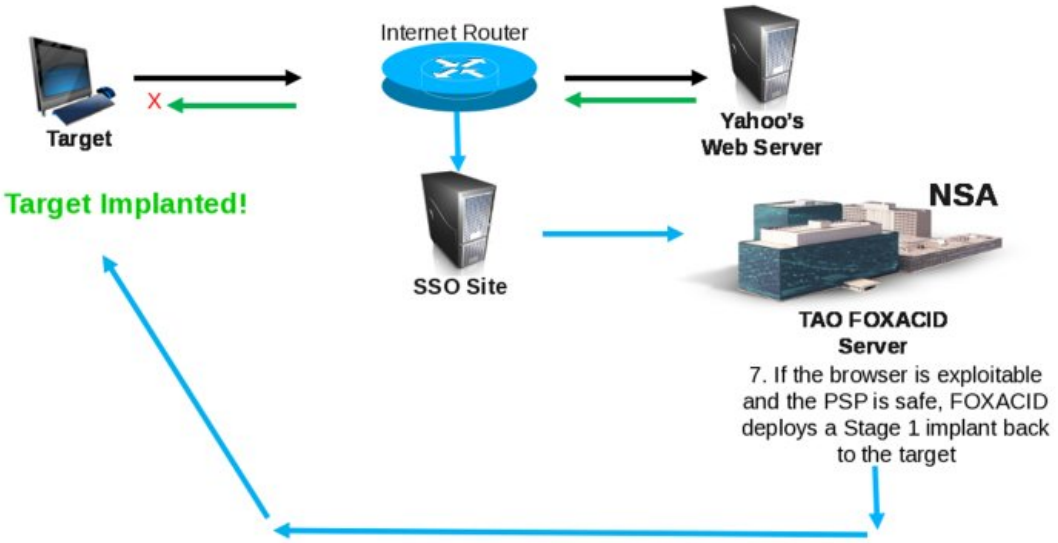
... NSA Quantum ...

nrw-unITS
IT-Sicherheit
Nordrhein-Westfalen

TOP SECRET//SI//REL USA, AUS, CAN, GBR, NZL

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



SDS Booz | Allen | Hamilton
SIGINT | Development | Support

TOP SECRET//SI//REL USA, AUS, CAN, GBR, NZL

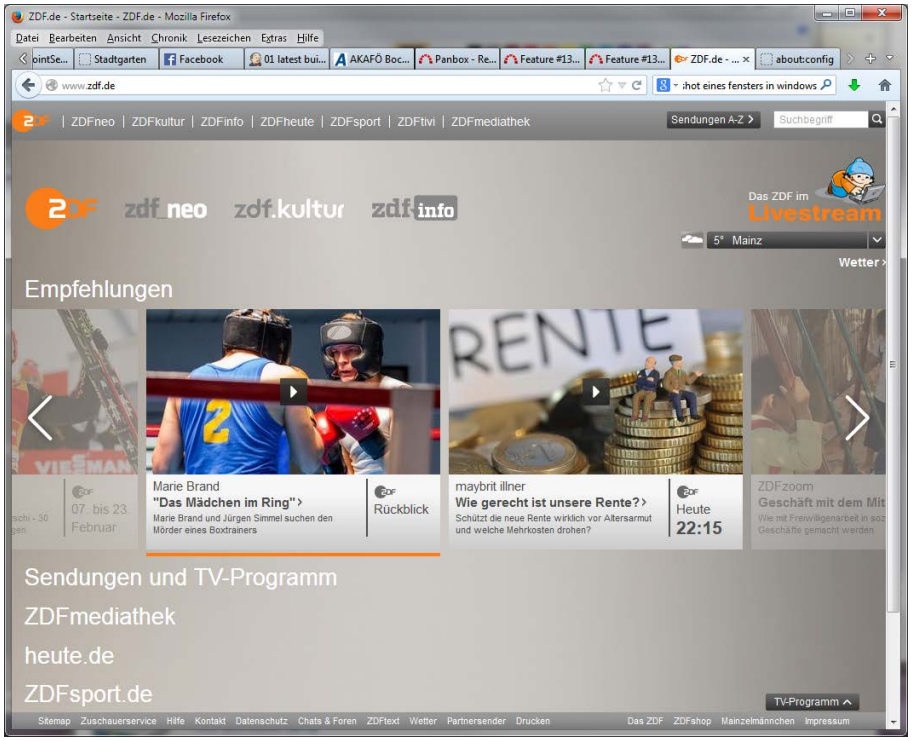
4

Sirrix AG
security technologies

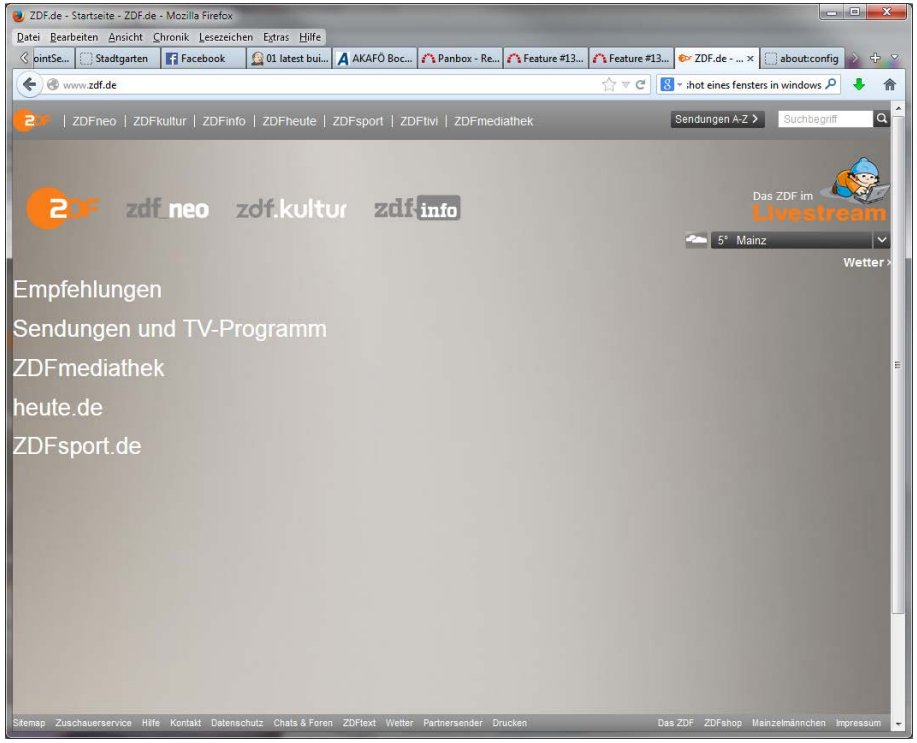
Aktive Inhalte allgegenwärtig

nrw-units
IT-Sicherheit
Nordrhein-Westfalen

- Mit JavaScript



- Ohne JavaScript



Sirrix AG
security technologies

Warum bergen Browser Gefährdungspotenziale?

- Browserkomplexität
  - Immer mehr Funktionalitäten werden im Browser integriert
  - Browser dienen nicht mehr nur der Darstellung von Web-Inhalten, sondern führen extern geladenen, ungesicherten Code aus
- Aktive Inhalte
  - Eines der Haupteinfallstore für Schadsoftware
  - Z. B. “Drive-by-Download”, Cross-Site-Scripting etc.
- Hohe Zahl infizierter Seiten
  - Können ohne Wissen der Betreiber Schadsoftware verbreiten
  - Insgesamt niedriger Security Patch-Level

Sicherheitsziel

- Schutz von **Arbeitsplatz** und **Intranet** vor Browserbasierten Angriffen aus dem Internet mit Fokus auf:
  - Vertraulichkeit der Daten und
  - Verfügbarkeit der IT-Infrastruktur

Lösungsansätze

- Schutz **des** Browsers
  - Browsereinstellungen, Browserpatches, Filterung von aktiven Inhalten, Proxy…
- Schutz **vor dem** Browser
  - Trennung Arbeitsplatz-PC / Browser PC
  - Remote Controlled Browser Systems (ReCobs)
  - Browser in the Box (BitBox)

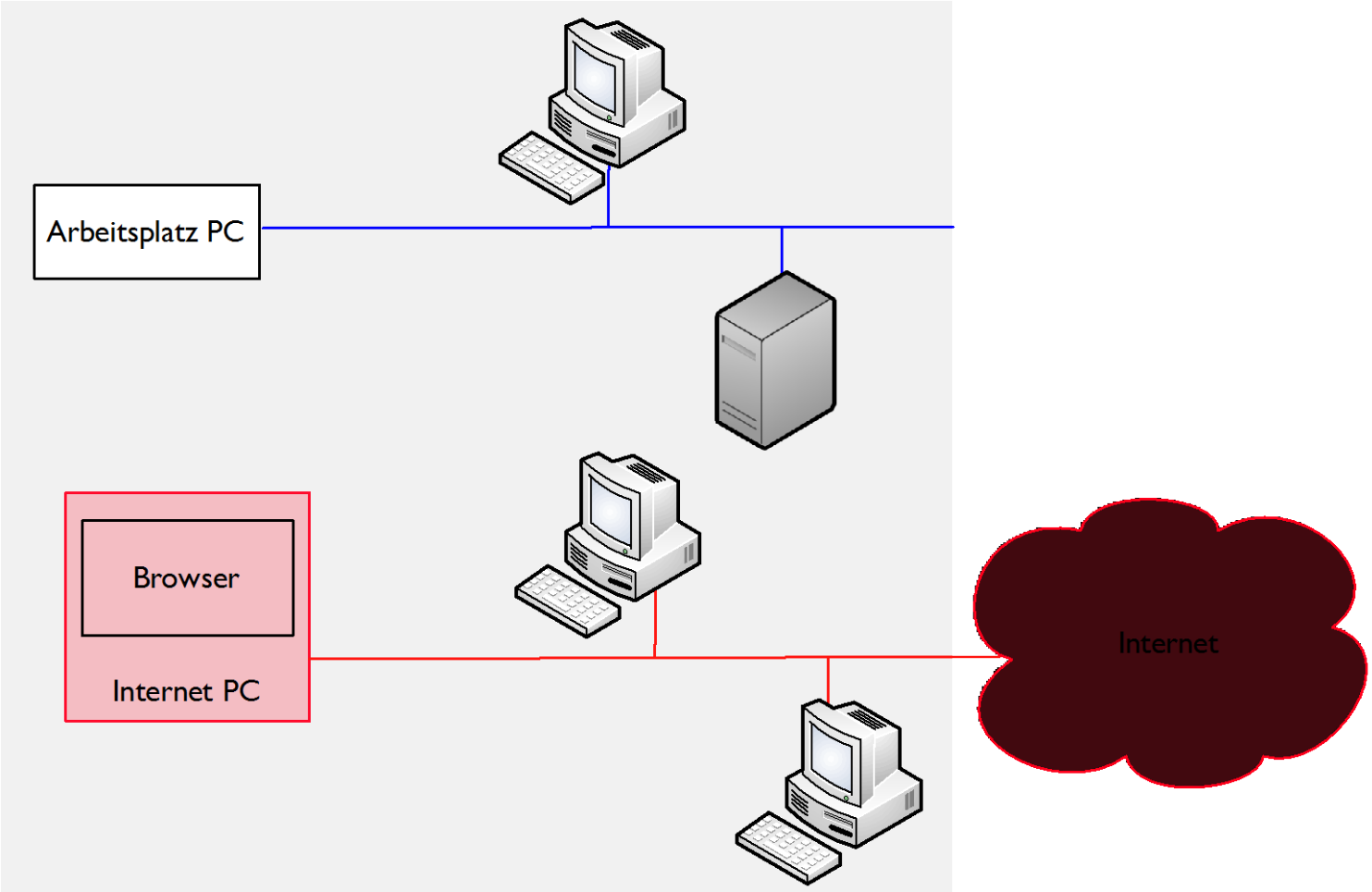
Kriterien an Sicherheitslösungen

- Sicherheit
- Webfunktionalität
- Benutzbarkeit
- Aufwand / Kosten
- Verfügbarkeit im Falle einer Infektion
- Mobiler Einsatz

Kein Web Zugang

- Pros:
  - Ultimative Sicherheit
- Cons:
  - Unmöglich für die meisten Firmen / Behörden

Physikalische Isolation



Physikalische Isolation

- Pros:
  - Hohe Sicherheit
  - Uneingeschränkte Webfunktionalität auf Internet PC
- Cons:
  - Schlechte Benutzbarkeit durch unterschiedliche PCs
  - Ungeeignet für mobilen Einsatz
  - Hohe Kosten durch Doppelausstattung
  - Hoher administrativer Aufwand durch Doppelausstattung
  - Hoher Aufwand bei Wiederherstellung von Infektion der Internet PCs

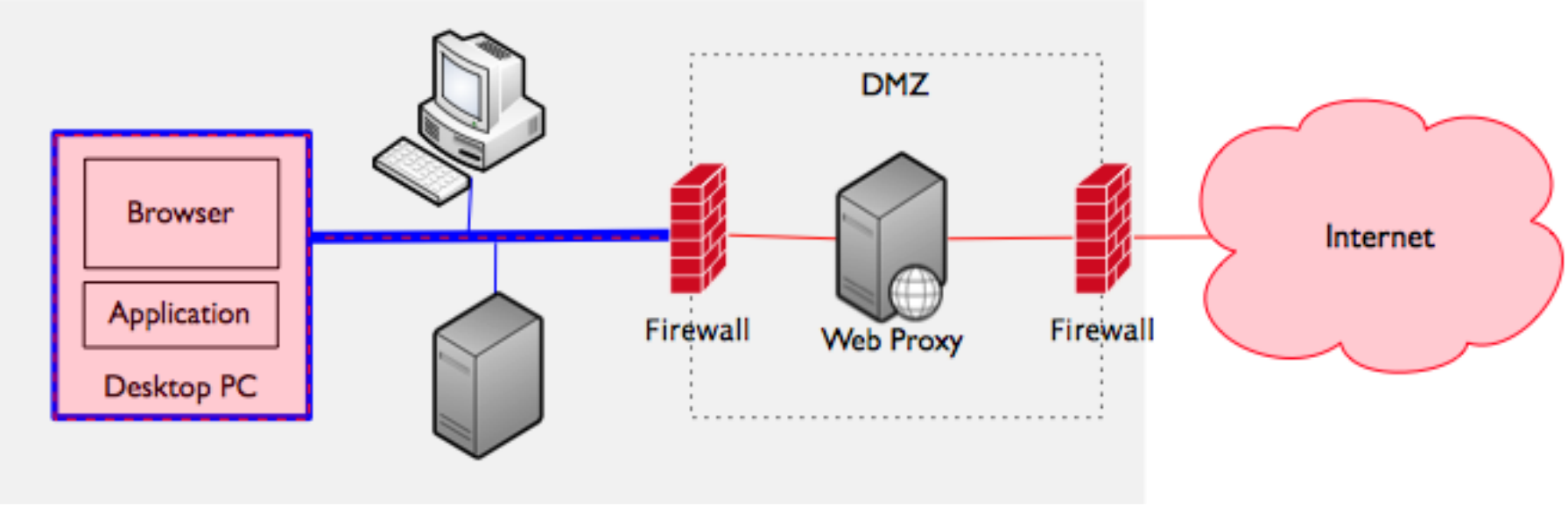
Browser Sicherheits Features

- Benutzung von Browsereinstellungen (e.g. JavaScript abschalten) und eingebauten Sandboxing

- Pros:
  - Keine zusätzlichen Kosten
  - Gute Benutzbarkeit
  - Uneingeschränkter mobiler Einsatz

- Cons:
  - Niedriges Sicherheitsniveau
  - Tradeoff: Sicherheit vs. Webfunktionalität
  - Sandboxing wird regelmäßig gebrochen
  - Bei Infektion ist gesamte Infrastruktur gefährdet

Proxy / Firewall

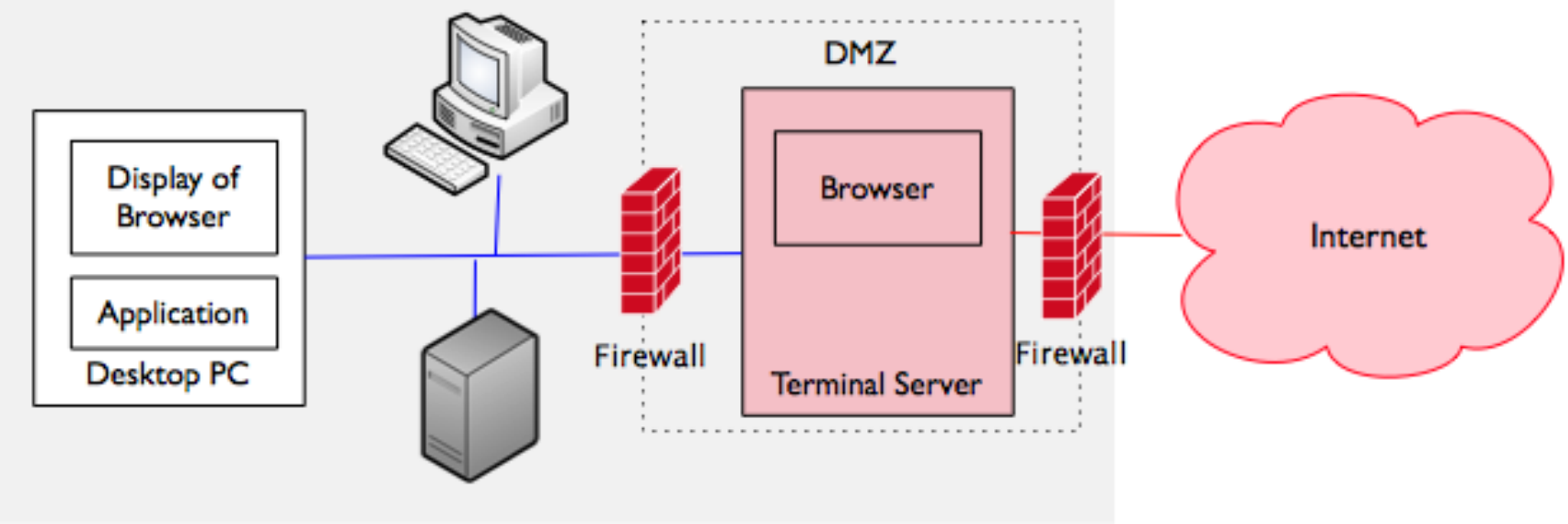


Proxy / Firewall

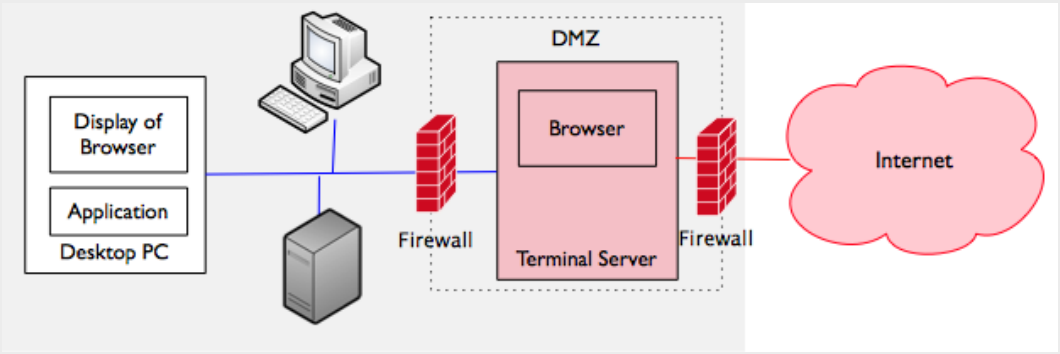
- Pros:
  - Zentrale Konfiguration
  - Leicht zu Benutzen
- Cons:
  - Tradeoff: Sicherheit vs. Webfunktionalität
  - Nicht effektiv gegen zero-day-exploits
  - Infektion gefährdet gesamte Infrastruktur

Remote Controlled Browsers

- Browser wird auf Terminal Server ausgeführt und am Arbeitsplatz PC lediglich angezeigt



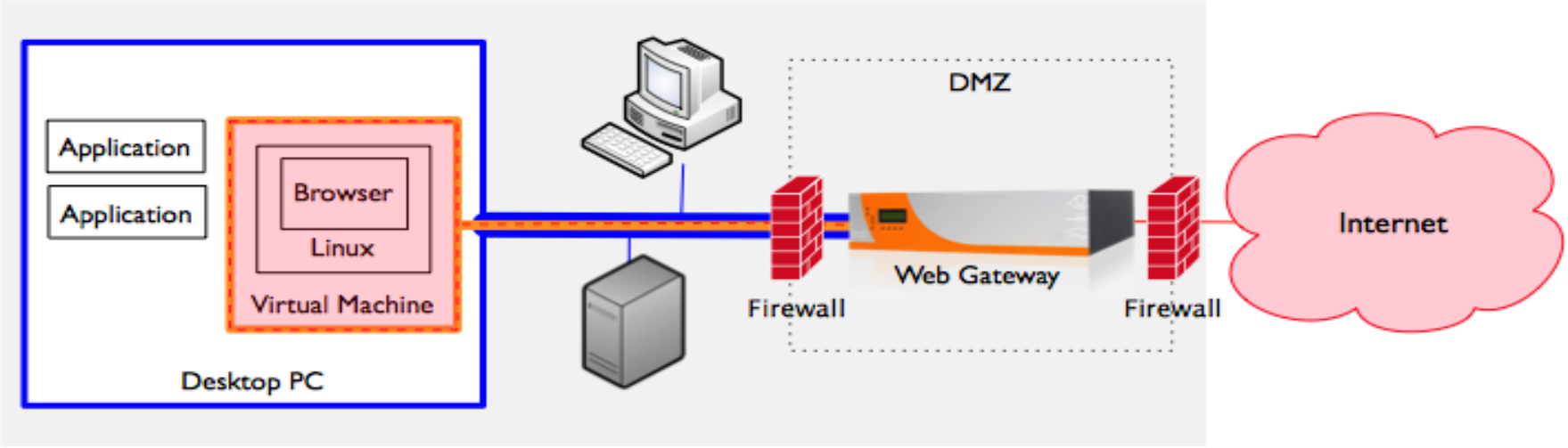
Remote Controlled Browsers



- Pros:
  - Hohe Sicherheit
  - Uneingeschränkte Webfunktionalität
  - Gute Benutzbarkeit
  - Gut geeignet für Terminal Server / Thin Client Infrastruktur
- Cons:
  - Zusätzliche Kosten für Terminal Server
  - Eingeschränkte Skalierbarkeit (Rechenleistung und Netzwerkbandbreite) durch zentrale Architektur
  - Ungeeignet für mobilen Einsatz durch hohe Bandbreiten
  - Interne Webportale brauchen separaten Browser

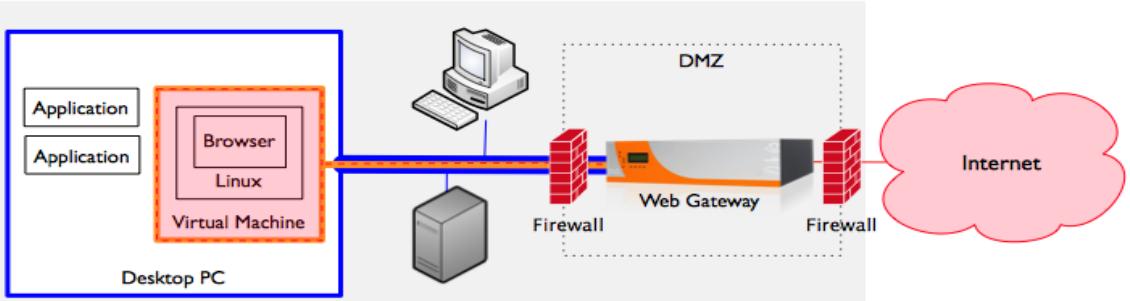
Browser in the Box

- Isolation des Browsers in **virtueller Maschine**
- Isolation des Netzwerks mit **VPN**



Sirrix AG
security technologies

Browser in the Box



- Pros:
  - Hohe Sicherheit
  - Uneingeschränkte Webfunktionalität
  - Wirtschaftlichkeit und Skalierbarkeit durch Nutzung von PC Ressourcen
  - Hohe Verfügbarkeit durch „Schnapschuss“ Funktionalität
  - Uneingeschränkter mobiler Einsatz
  - Niedrige Kosten bei Einsatz eines Standardproduktes
  - Gut geeignet für klassische Client / Server Infrastruktur
- Cons:
  - Interne Webportale brauchen separaten Browser

Zusammenfassung

- Browser sind verwundbar und werden es bleiben
- Aktive Inhalte sind unverzichtbar in modernen Webseiten
- Perimeter Schutz und Browser-Härtung bleiben verwundbar gegen zero-day-exploits
- Effektiver Schutz nur durch Isolation von Browser und Internetzugriff vor dem Intranet und dem Arbeitsplatz PC

Gibt es noch Fragen?

nrw·uniTS
IT-Sicherheit
Nordrhein-Westfalen

Autor:
Dr. Norbert Schirmer / Head of Endpoint Security and Projects

E-Mail:
n.schirmer@sirrix.com

Unternehmen:
Sirrix AG
Lise-Meitner-Allee 4
40801 Bochum

Web:
www.sirrix.de

Vielen Dank für Ihre Aufmerksamkeit!

Ministerium für Wirtschaft, Energie, Industrie, Mittelstand und Handwerk des Landes Nordrhein-Westfalen

Sirrix AG
security technologies

EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds für regionale Entwicklung