



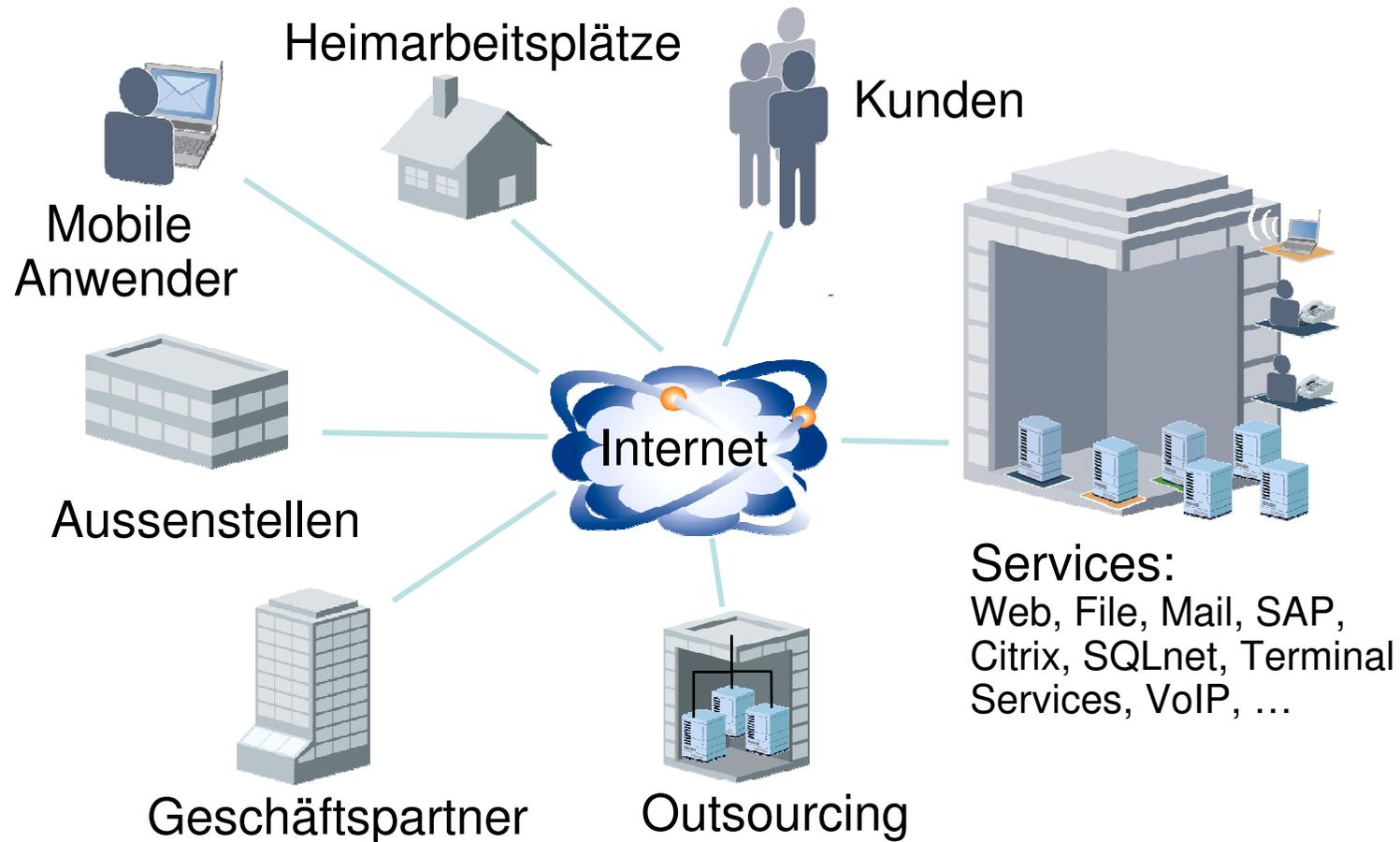
INTEGRALIS
Your Trusted Security Partner

SSL VPN

www.integralis.de

Hintergrund

- Wie erfolgt heute der Zugriff auf die Ressourcen?



Problematik

- Unternehmen bauen sich eine Vielzahl von Gateways auf
 - Einwahlrouter, VPN Gateways (meist IPSEC), Webserver/ Portale, Reverse Proxies, Citrix (NFuse/WebView + Secure Gateway), Terminalserver, ...
- Diese verursachen hohe Kosten
 - Initial: Kosten Client/Server, Thema Sicherheit/ Hochverfügbarkeit
 - Operating: Kosten Maintenance, Admin Knowhow
- Nur Teilaspekte werden adressiert bzgl.
 - Client/Server-Sicherheit
 - Flexibilität
 - Integrationsfähigkeit
- Sind auch neue Anforderungen des Unternehmens abbildbar?

Der Bedarf unserer Kunden

- Sicherer und flexibler Zugriff unabhängig von Gerät und Ort
 - PDAs, Internet-Café, FlughafenTerminal, Partnernetze, ...
- Besserer Schutz auf Client- und Server-Seite
 - Durchsetzen von Sicherheitsrichtlinien auf externen Clients
 - Kontrolle auf Applikationsebene/ Anwendungsebene
- Unterstützung alternativer Betriebssysteme
 - Windows (Mobile Edition), Linux, MacOS
- Nachvollziehen + Zuordnen von Zugriffen
 - Anforderungen aus Security Guidelines/ Standards wie SOX, Basel II, FDA 21 CFR Part11

Geht das schon heute?

- Ja, mit SSL VPN sind die Anforderungen umsetzbar!
- K.O. für andere Technologien?
 - RAS/ Dial in:
 - Keine Verschlüsselung, keine Security, keine Flexibilität
 - IPSEC:
 - bietet funktionell nur eine Teilmenge von SSL VPN
 - Mangel an Flexibilität bzgl. des Zugriffs, kein clientless VPN
 - kein Schutz auf Anwendungsebene
 - Unterstützung alternativer Betriebssysteme sehr dürftig
 - TerminalServices/ Citrix/ WebServices:
 - Keine Client Security
 - Begrenzte Sicherheit auf Anwendungsebene

Weiterer Nutzen durch SSL VPN

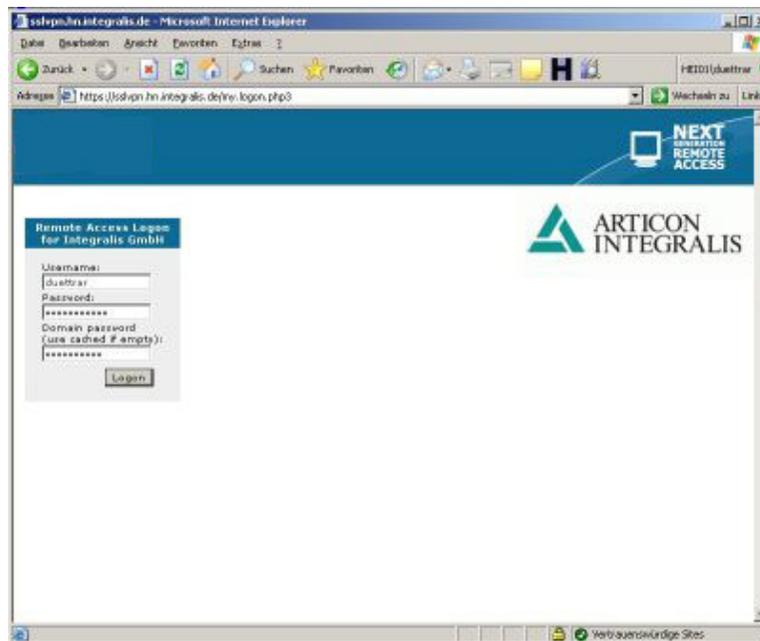
- Sehr wirtschaftliche Lösung
 - Geringe Anschaffungskosten
 - Infolge der Konsolidierung von Services wird Hardware, Software und Maintenance benötigt
 - Aus technischer Sicht simpler Ausbau als globale Lösung
- Geringer Aufwand bei Betrieb und Implementierung
 - Vereinfachen der Netzwerkstruktur durch zentralen Übergangspunkt
 - Zugriffe erfolgen oftmals Clientless, Unterstützung bei Rollout
- Benutzerfreundliche Bedienung
 - Hohe Benutzerakzeptanz
- Flexible Unterstützung neuer Geschäftsprozesse

Strategie

- Vereinfachen der Netzwerkinfrastruktur durch Konsolidierung
 - SSL VPN als zentraler Übergangspunkt für Client-Zugriffe
- Ausweiten der Sicherheit bis zum Endpunkt
 - Durchsetzen von Sicherheitsrichtlinien auf externe Clients
- Sicherer Zugriff unabhängig von Ort und Gerät

Technische Lösung – SSL VPN

- Funktionsweise aus Sicht des Benutzers
 - Benutzer melden sich per Webbrowser am Gateway an (optional: mit Token bzw. Zertifikat)



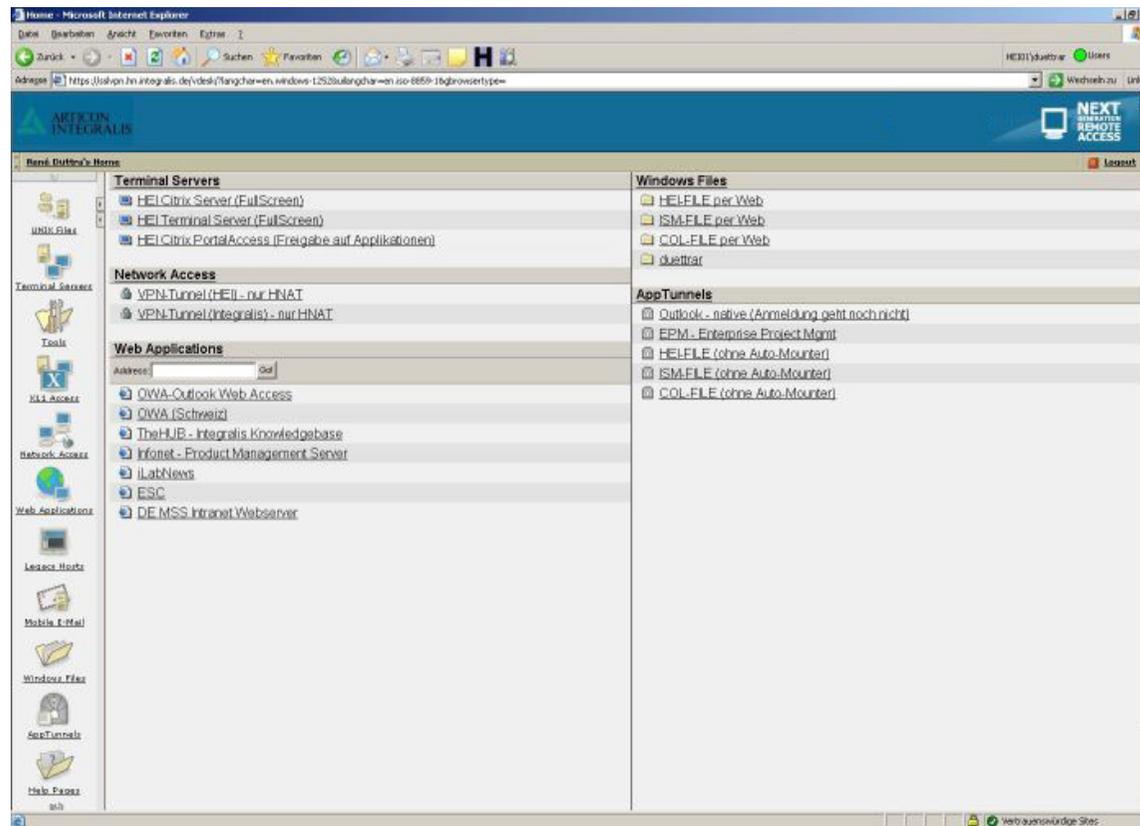
Smartcard



Token

Technische Lösung (cont.)

- Nach der erfolgreiche Anmeldung erhält der Benutzer Zugriff auf die Unternehmensressourcen



Betriebliche Aspekte

- Zugangssysteme werden häufig international genutzt – ist ein 24/7 Helpdesk notwendig?
- Kann eine extern gemanagte Lösung Ihren Betrieb unterstützen? Welchen Service stellen Sie sich vor?
- Die Remote Access Lösung wird zentraler Bestandteil der IT-Umgebung – welche SLAs benötigen Sie?

Wir können Sie unterstützen!

- Technische Präsentation in Ihrem oder unserem Haus
- Technische Konzepte
- Implementierung, Rollout und Migration
- Training
- Kontakt zu Referenzkunden