Aufbau einer einfachen und sicheren Remoteverbindung für den Zugriff auf Zentrale Systeme im Hessischen Ministerium für Wissenschaft und Kunst

Dokumentation der betrieblichen Projektarbeit von

Mathias Axtmann

zum Erlangen des Abschlusses als
Fachinformatiker / Systemintegration

TECHNISCHE UNIVERSITÄT DARMSTADT

Durchgeführt am:

Hessischen Ministerium für Wissenschaft und Kunst
Rheinstraße 23 - 25
65185 Wiesbaden

HESSEN

Mit der freundlichen Bitte um Benotung.

Inhaltsverzeichnis

Inhaltsverzeichnis		II
Persönliche Erklärung des Prüfungsteilnehmers		III
1	Projektbeschreibung aus Kundensicht	1
1.1	Das Projektumfeld	1
1.2	Ausgangssituation	1
1.3	Projektziele	1
1.4	Projektschnittstellen	2
2	Machbarkeitsstudie	2
3	Ressourcen und Ablaufplanung	3
3.1	Personalplanung	3
3.2	Sachmittelplanung	3
3.3	Kosten- Nutzenplanung	4
4	Ablaufplan	6
5	Projekt Kick-Off	7
6	Projektdurchführung	8
6.1	Projektmarketing	8
6.2	Entscheidungsfindung	8
6.3	Beschaffung	8
6.4	Installation	8
6.5	Konfiguration der Software	8
6.6	Funktionstest	9
6.7	Risikoanalyse	10
6.8	Übergabe der Projektergebnisse	11
7	Projektergebnis	12
7.1	Soll-Ist-Vergleich	12
7.2	Abweichungen	12
8	Fazit	13
Literaturverzeichnis		IV
Abkürzungsverzeichnis		V
Abbildungsverzeichnis		VI

Persönliche Erklärung des Prüfungsteilnehmers

Ich versichere durch meine Unterschrift, dass ich die betriebliche Projektarbeit und die dazugehörige Dokumentation selbstständig in der vorgesehenen Zeit erarbeitet habe.

Ebenso bestätige ich, dass ich bei der Erstellung der Dokumentation meiner Projektarbeit weder Teile, noch vollständige Passagen, aus Projektarbeiten übernommen habe, die bei der prüfenden oder einer anderen Kammer eingereicht wurden.

_____	_____
Ort, Datum	Mathias Axtmann

Privatanschrift Auszubildender

Mathias Axtmann
64289 Darmstadt

Tel: 0611 32-3255 (HMWK)
E-Mail: mathias.axtmann@hmwk.hessen.de

Ausbilder (Projektverantwortlicher)

Dipl.-Inform. Klaus Balser
Technische Universität Darmstadt
Petersenstraße 30
64287 Darmstadt

Tel: 0611 32-3533 (HMWK)
Tel: 06151 16-6952 (TU Darmstadt)
E-Mail: klaus.balser@hmwk.hessen.de

Projektleiter des IT-Ausbildungsverbundes

Michael Starke
Technische Universität Darmstadt
Petersenstraße 30
64287 Darmstadt

Tel: 06151 16-6953
Fax.: 06151 16-3050
E-Mail: starke@hrz.tu-darmstadt.de

1 Projektbeschreibung aus Kundensicht

In den folgenden Abschnitten werden die Anforderungen des Kunden an das Projekt und die bestehende Umgebung näher erläutert.

1.1 Das Projektumfeld

Das Hessische Ministerium für Wissenschaft und Kunst (HMWK) befindet sich in Wiesbaden und ist mit seinen 250 Mitarbeitern das kleinste Ministerium des Landes Hessen. Die Aufgaben des Ministeriums erstrecken sich auf das Hochschulwesen, wissenschaftliche Forschungs- und Kultureinrichtungen. Die Informationstechnik (IT) wird seit 1998 über einen Outsourcing-Vertrag zwischen dem HMWK und dem Hochschulrechenzentrum (HRZ) der Technischen Universität Darmstadt (TU Darmstadt) geregelt.

Für die IT ist derzeit Herr Klaus Balser mit einem Angestellten und zwei Auszubildenden im HMWK zuständig.

Folgende Hardware-Komponenten sind an jedem Arbeitsplatz am HMWK vorzufinden: Personal Computer (PC), 19“-Liquid-Crystal-Display-Monitor (LCD-Monitor), Schwarz-Weiß-Laserdrucker.

Als Software kommt auf den Rechnern zum Einsatz: Microsoft Windows XP, Microsoft Office 2003, Adobe Acrobat Reader, WinZip, Free PDF und Antivirusprogramm Sophos Endpoint Security & Control.

Momentan werden weitere 31 Netzwerkdrucker, 35 Notebooks und acht Server von der IT verwaltet. Im Hause ist eine strukturierte Kategorie 6 (CAT 6) Verkabelung vorzufinden. Jedes Stockwerk verfügt über einen Etagenverteiler mit mindestens einem Switch und einem Patchfeld. Diese sind untereinander über Lichtwellenleiter (LWL) verkabelt und zentral im Serverraum verbunden.

Die Hessische Zentrale für Datenverarbeitung (HZD) stellt den Zugang zum Corporate Network (HCN), auch Hessennetz genannt, eine 100-MBit-Standleitung bereit. Über dieses Netz laufen alle zentralen Landesdienste wie z.B. das Zentrale Mailing (ZEM), eGesetz, eKIS, Hessische Dokumentverwaltung (HeDok).

Der Zugang zum Wide Area Network (WAN) wird über eine weitere 100 MBit/s schnelle Standleitung durch die Arbeitsgruppe Metropolitan Area Network Darmstadt (AG MANDA) ermöglicht.

1.2 Ausgangssituation

In unserer Arbeitswelt hat sich der Begriff "Mobilität“ einen festen Platz erobert. Hiervon sind auch Ministerien und Behörden nicht ausgenommen. Deshalb wird eine "Plug and Work“-Lösung für eine einfache und sichere Remoteverbindung für den Zugriff von entfernten Standorten auf die zentralen Systeme gesucht, um den Mitarbeitern des Hessischen Ministerium für Wissenschaft und Kunst diese "Mobilität" zu ermöglichen.

1.3 Projektziele

Ziel des Projektes ist eine für den Benutzer einfache und sichere zu verwendende Remote Umgebung aufzubauen. Dadurch wird das Arbeiten von entfernten Standorten aus möglich. Zusätzlich soll dieses Projekt eine Kostenersparnis gegenüber der bisherigen verwendeten Remote Zugriffs-Software bringen.

1.4 Projektschnittstellen

Abhängig von den einzelnen Projektphasen ergaben sich verschiedene Ansprechpartner. Für das Festsetzten des Budgetrahmens ist Herr Klaus Riehl und Herr Jan-Hendrik Krumme aus dem Referat I verantwortlich. Die Beschaffung der Software fällt in den Zuständigkeitsbereich von Frau Roswitha Mattzatz aus dem Referat I. Mein Ausbilder und Vorgesetzter, Herr Klaus Balser, ist für alle technischen Fragen und Probleme zuständig. Weiterhin stehe ich mit Herrn Michael Bleicher von der Firma Giritech für die Integration der Software in Kontakt. Herr Markus Stögbauer von der MANDA steht mir für die Einrichtung der Demilitarisierten Zone (DMZ) zur Verfügung.

2 Machbarkeitsstudie

Mit einer Machbarkeitsstudie soll ermittelt werden, ob das Projekt überhaupt seinen Zweck erfüllt, sowie die Untersuchung von Rahmenbedingungen und Lösungsmöglichkeiten. Nachfolgend wird dies in technische, organisatorische und wirtschaftliche Machbarkeit unterteilt.

Wirtschaftliche Machbarkeit

Für die Realisierung dieses Projektes wurden 3.000 € zur Verfügung gestellt. Dieses Budget ist nach einer Analyse bzw. Recherche für die Hard- und Software Neuanschaffung ausreichend.

Organisatorische Machbarkeit

Einer der wichtigsten Aufgaben in der Organisation von Projekten für den Projektzeitraum ist die Personalplanung. Deshalb wurde sichergestellt, dass alle Ansprechpartner zur Verfügung stehen. Um die Implementierung der Lösung so schnell wie möglich zu verwirklichen, wird der Auszubildende von anderen Projekten für den Zeitraum, der Projektdurchführung freigestellt. Ein verbindlicher Zeitrahmen für meine Projektarbeit wurde nach Rücksprache mit den betreffenden Ansprechpartnern meiner Projektschnittstellen festgelegt.

Technische Machbarkeit

Im Moment werden 25 Telearbeitsplätze über die Software Cisco VPN im HMWK betrieben. Cisco VPN hat annähernd die gleichen technischen Anforderungen wie die in meinem Projekt verwendete Software. Das bedeutet, dass die technische Machbarkeit sich direkt ergibt. G/On wurde ausgewählt weil es benutzerfreundlich, wartungsarm, sicher und schnell ist. Es ist von meinem Vorgesetzten gewünscht, dass der G/On Server, der zur Authentifizierung und zur Einwahl dient, in einer Demilitarisierten Zone (DMZ) steht. Die Netzstruktur des HMWK besitzt keine DMZ. Nach Absprache mit der AG MANDA, die für die Netzstruktur des Hauses verantwortlich ist, wurde beschlossen, diese Arbeiten vorzuziehen und eine DMZ einzurichten. Damit ist die technische Machbarkeit sichergestellt.

Risiken

Es bestehen keine besonderen Risiken im Verlauf der Projektarbeit, da alle internen Organisationsaufgaben, Hardwarebeschaffungen und Verkabelungen problemlos innerhalb der vorgegebenen Zeit erledigt werden können. Meine Ansprechpartner bei den unterschiedlichen Projektschnittstellen stehen mir im angegebenen Projektzeitraum zur Verfügung und auch die Lieferfrist für die G/On Produkte, welche eine Woche beträgt, kann eingehalten werden.

3 Ressourcen und Ablaufplanung

„Ein Projekt darf nie kürzer und günstiger als geplant sein.“

Henri de Saint-Simon (1760-1825)

Nachfolgend werden die Personalplanung, Sachmittelplanung und Kosten-Nutzenplanung separat betrachtet und aufgeschlüsselt.

3.1 Personalplanung

Bei der Personalkostenplanung sind die Zeiten des Auszubildenden, sowie die Stunden für die Schulung der Mitarbeiter und die Stunden für die Gespräche mit dem Vorgesetzten aufgeführt.

Personalplanung			
Anzahl	Posten	Einzelpreis	Gesamtpreis
35	Zeitstunden Auszubildender	25,00 €	875,00 €
5	Zeitstunden Gespräche mit Kollegen	45,00 €	225,00 €
5	Zeitstunden Gespräche mit Vorgesetzten	55,00 €	275,00 €
2	Schulung der Mitarbeiter	195,00 €	390,00 €
	Gesamtkosten Brutto		**1.765,00 €**

Abb. 01: Personalplanung

3.2 Sachmittelplanung

Der Hauptteil der Kosten bezieht sich auf die Anschaffung der Software. Um die Kosten entsprechend niedrig zu halten, wurde ein Hewlett Packard DL360 G5 in Betrieb genommen, der zur damaliger Zeit bei uns im Hause als Remote Installation Services (RIS) Server genutzt wurde und durch einen neuen ersetzt werden sollte.

Sachmittelplanung			
Anzahl	Posten	Einzelpreis	Gesamtpreis
1	Server Hewlett Packard – DL 360 G5	0,00 €	0,00 €
1	G/On 5 Server - Basisaussstattung	0,00 €	0,00 €
5	G/On 5 User - Access License	100,00 €	500,00 €
5	G/On 5 Token – Access License	150,00 €	750,00 €
5	Maintenance für G/On 5 Lizenzen - 20 % auf die Lizenz Preise		250, 00 €
5	G / On USB Access Key, H3 1 GByte	66,00 €	330,00 €
	Zwischensumme:		1.830,00 €
	Zzgl. 19 % MwSt.		347,70 €
	Gesamtkosten		**2.177,70 €**

Abb. 02: Sachmittelplanung

3.3 Kosten-Nutzenplanung

Durch die neue Remotelösung G/On sind Kosteneinsparungen von immenser Größe bei jedem einzelnen User zu realisieren. Im Folgenden wird der Vergleich in zwei Tabellen aufgezeigt.

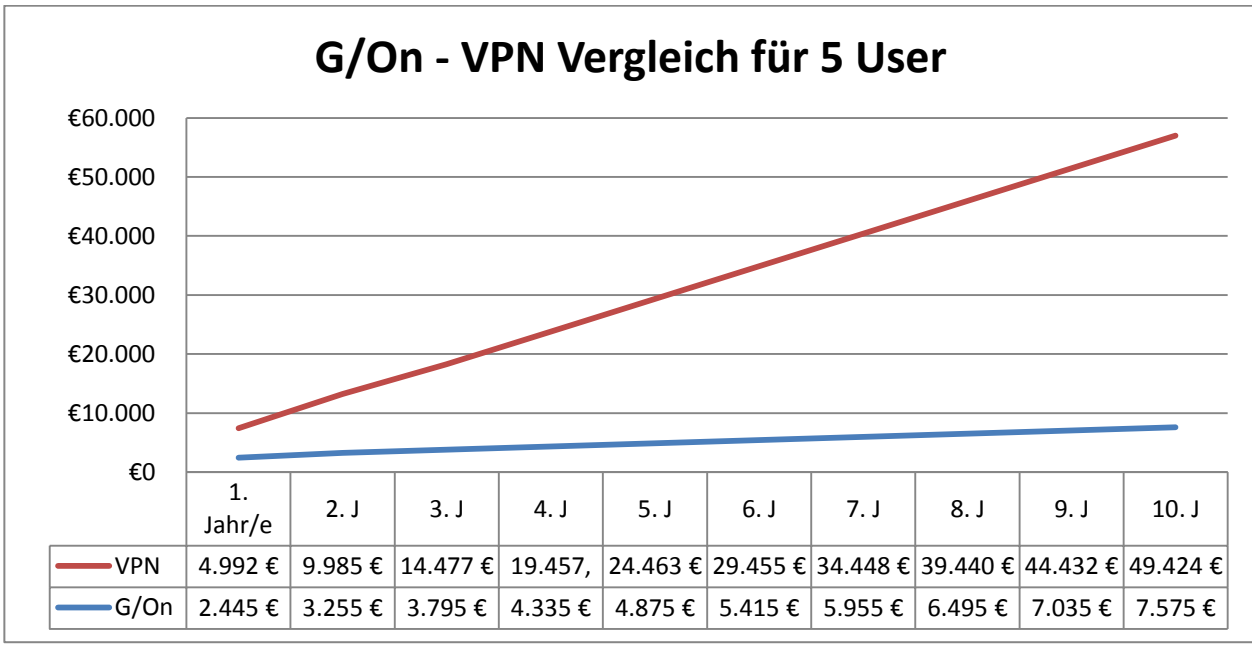
Virtual Private Network – Kosten	
Monatliche Gebühr für 1 Client Zugang Für 24 Monate, 24 x 28 €	28,00 € **672,00** €
HZD VPN Einrichtung – einmalig pro User	200,00 €
HMWK IT – 1 Std. VPN Einrichtung, Dokumentation einmalig	45,00 €
HMWK IT – 1 Std./Monat pro User für VPN Betreuung, Updates Für 24 Monate, 24 x 45 (1Std./Monat)	45,00 € **1.080,00 €**
Zwei Jahre, ein VPN User: **Zwei Jahre, fünf VPN User**	1.997,00 € **9.985,00 €**

Abb. 03: VPN – Kosten

G/On – Kosten	
G/On Access License einmalig	100,00 €
G/On 5 Token – Access License einmalig	150,00 €
Maintenance für G/On 5 Lizenzen - 20 % auf die Lizenz Preise	50,00 €
G/On USB Access Key, H3 1 GByte	66,00 €
G/On Client Grundkonfiguration 15 min.	11,25 €
HMWK IT - User Client Dokumentation einmalig	45,00 €
HMWK IT - Installation G/On Server 4 Std. Konfiguration, Dokumentation einmalig	180,00 €
Laufende Kosten: G/On Client Packet Anpassung, Server Updates 1 Std. / Monat Für 24 Monate, 24 x 45 (1Std/Monat)	 45,00 € 1.080,00 €
Ein G/On User für 2 Jahre. Inklusive. 19 %MwSt. Fünf G/On User für 2 Jahre +45 € 1Std./Monat für Client Anpassung, Server Updates. Zwei Jahre, fünf G/On User inklusive einmalige Kosten	435,00 € 2.175,00 € 3.255,00 € 3.525,00 €
Zwei Jahre, ein G/On User **Zwei Jahre, fünf G/On User**	435,00 € **3.255,00 €**

Abb. 04: G/On – Kosten

Wie auf beiden voranstehenden Rechnungen zu sehen, ergeben sich völlig unterschiedliche Kosten. Die momentan eingesetzte VPN Technik enthält vor allem laufende Kosten die pro Monat anfallen. Mit G/On entstehen fast ausschließlich einmalige Kosten. Deshalb kommt man über zwei Jahre gerechnet auf eine Kostenersparnis von 84%! Das folgende Diagramm verdeutlicht nochmals den Kostenunterschied.



	1. Jahr/e	2. J	3. J	4. J	5. J	6. J	7. J	8. J	9. J	10. J
VPN	4.992 €	9.985 €	14.477 €	19.457,	24.463 €	29.455 €	34.448 €	39.440 €	44.432 €	49.424 €
G/On	2.445 €	3.255 €	3.795 €	4.335 €	4.875 €	5.415 €	5.955 €	6.495 €	7.035 €	7.575 €

Abb. 05: G/On / VPN – Kosten

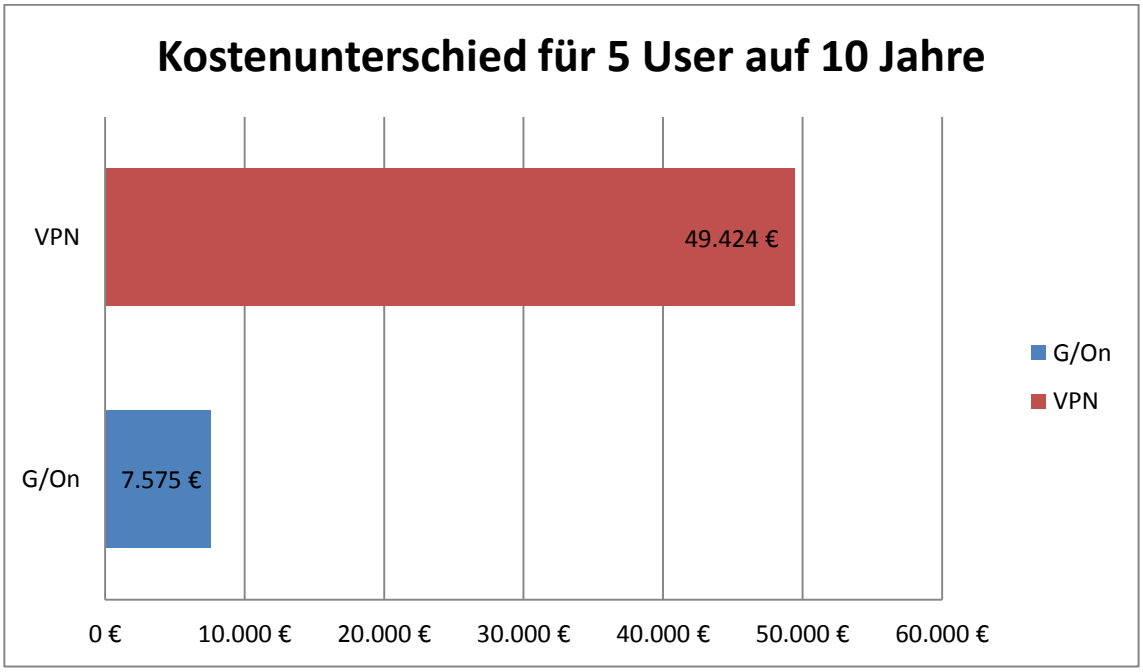


Abb. 06: G/On – VPN Kosten Unterschied 5 User/10 Jahre

4 Ablaufplan

Der Ablaufplan wird in einem Gant Diagramm dargestellt. Ich möchte darauf hinweisen, dass Lieferzeiten und mögliche Lieferverzögerungen nicht mit einberechnet wurden. Ich habe die Lieferzeit des Produkts bewusst so gewählt, dass es in die Berufsschulzeit gefallen ist und somit keine Verzögerungen in der Projektdurchführung zu erwarten war.

Kennung	*Aufgabenname*	*Anfang*	*Abschluss*	*Dauer*
1	Analye des Ist - Zustandes	14.03.2011	14.03.2011	2h
2	Soll-Konzeption definieren	14.03.2011	14.03.2011	2h
3	Angebot einholen und Beschaffung der benötigten Hardware	15.03.2011	15.03.2011	1,5h
4	Planung der Umsetzung in die IT-Infrastruktur	15.03.2011	15.03.2011	2,5h
5	Aufbau/Installation der Hardware/ Software Komponenten	16.03.2011	16.03.2011	5h
6	Konfiguration, Einrichtung und erste Funktionstests	17.03.2011	17.03.2011	3h
7	Integration der Umsetzung in den Betriebsablauf	17.03.2011	18.03.2011	4h
8	Erstellen der Kundendokumentation	18.03.2011	18.03.2011	2,5h
9	Schulung der Mitarbeiter	18.03.2011	18.03.2011	2,5h
10	Projektdokumentation	17.03.2011	18.03.2011	10h

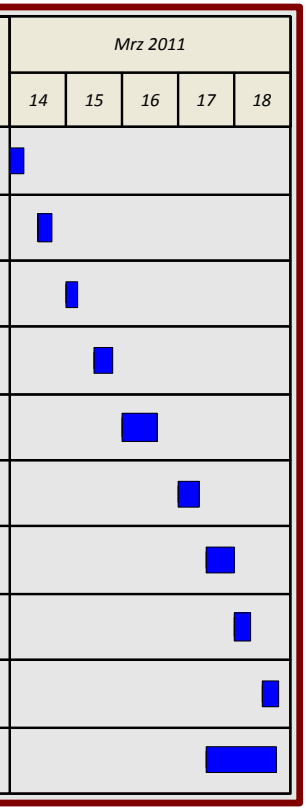


Abb. 07: Ablaufplan

5 Projekt Kick-Off

Das Projekt wurde in einer Teamsitzung nochmals mit allen Kollegen der IT besprochen. Folgende Punkte wurden dabei abgeklärt:

- Klarheit über übergeordnete Projektziele, Ziele der aktuellen Projektphase und erwartete Resultate
- Nutzen des Projekts für das Unternehmen
- Konkretes Vorgehen und anzuwendende Methoden

Es wurde entschieden, dass dieses Projekt zunächst für die IT-Administratoren im HMWK dient und nicht für die User im HMWK. Das liegt daran, dass das Projekt zeitlich auf 35 Stunden beschränkt ist und die Einrichtung eines Terminal-Servers den Zeitrahmen sprengen würde. Dies bedeutet, dass der Arbeitsplatz-Rechner für die HMWK Administratoren per „Wake on LAN“ hochgefahren und anschließend eine Remoteverbindung aufgebaut wird.

6 Projektdurchführung

6.1 Projektmarketing

Mein Vorgesetzter sowie die IT-Mitarbeiter wurden täglich über den Fortschritt des Projektes per E-Mail-Verteiler auf dem Laufenden gehalten. In einem digitalen Ordner wurde der aktuelle Fortschritt festgehalten. In der wöchentlichen Teamsitzung sind Änderungen bzw. Verbesserungsvorschläge diskutiert worden.

6.2 Entscheidungsfindung

Das Produkt G/On wurde vorher schon im HMWK als Pilotprojekt getestet. Da es mit G/On und den resultierenden positiven Erfahrungen keinerlei Probleme gab, wurde es direkt für meine Abschlussarbeit weiter verwendet. Deshalb hat keine Entscheidungsfindung stattgefunden.

6.3 Beschaffung

Wie bereits beschrieben, wurde um Kosten einzusparen, ein alter Server von unserem Hause verwendet. Deshalb musste nur die G/On Software und die dazugehörigen G/On USB Token beschafft werden. Das Angebot der Firma Giritech wurde von mir überprüft, anschließend von meinem Vorgesetzten Herrn Klaus Balser genehmigt und dann an Frau Roswitha Mattzatz zur Beschaffung freigegeben.

6.4 Installation

Bevor die G/On Software auf dem Server installiert werden konnte, musste dieser zunächst eingebaut, installiert und konfiguriert werden. Als Betriebssystem kommt Windows Server 2008 R2 zum Einsatz. Die G/On Server Setup Datei weist keinerlei Besonderheiten auf. Sie kann jederzeit per Authentifizierung auf der Homepage heruntergeladen werden. In der Installation selbst wird lediglich der Pfad angegeben und wie üblich die Dateien dorthin kopiert.

6.5 Konfiguration der Software

Nach der Installation gibt es zwei neue Symbole, die auf dem Desktop des Servers zu finden sind. Als erstes beginnt man mit der Verknüpfung „G/On Server Configuration“. Hier werden zunächst alle notwendigen grundlegenden Funktionen und Dienste konfiguriert. Das wäre z.B. die Angabe über den Fully Quallified Domain Name (itshessen.hessen.de) oder die Ports die verwendet werden. Die Eingaben werden einmalig vorgenommen und werden im laufenden Betrieb nicht verändert.

Die zweite Verknüpfung lautet „G/On Server Management“. Hier werden alle wichtigen Funktionen wie Rechte, Authentifizierung, Gruppen und Menü Strukturen erstellt und definiert. Das Management ist sehr übersichtlich gestaltet und per „Drag and Drop“ konfigurierbar. Die G/On USB Token sind mit Nummern versehen. Im Management Menü wird diese Nummer auf den User gezogen um ihn für den Zugang zu berechtigen.

6.6 Funktionstest

„Der erste Test, ist meistens kein Fest.“

Autor unbekannt

Der Funktionstest ist für ein Projekt extrem wichtig. Im Grunde zeigt sich hier, ob das Projekt erfolgreich war. Einige Punkte mussten vor dem Test noch beachtet werden. Zunächst wird der TCP Port 443 am G/On Server freigeschaltet. Vor der Registrierung auf dem Server muss die Client-Software auf den G/On Sticks installiert werden. Dabei muss Wake on LAN auf allen Rechnern aktiviert sein. In einem Administrationsvideo habe ich alle Vorkehrungen nochmals genau dargestellt. Nachdem diese erfüllt waren, gab es keinerlei Probleme bei der Verbindung. In einem Funktionstest wurde die Kommunikation mit dem Server und dem Client über das Internet getestet, sowie die Remote Desktop Verbindung auf den Rechner im HMWK. Abbildung 8 stellt die Testmatrix nochmal genauer da. Dabei gelten alle Messpunkte gleichermaßen als „kritisch“.

Funktionstest – G/On Zugang		
Was wird getestet?	**Positiv**	**Negativ**
Verbindung zum G/On Server im HMWK	X	
G/On Menü Struktur richtig anzeigen	X	
Arbeitsplatz im HMWK per Wake on LAN hochfahren	X	
Remote Desktop Verbindung herstellen	X	
Automatische Windows Anmeldung	X	
Zugriff auf Intranet, E-Mail, Fileserver, HeDok	X	
Rechner Remote ausschalten?	X	

Abb. 08: Funktionstest – G/On Zugang

Der Zugriff auf den Rechner im HMWK lief tadellos. Ein Geschwindigkeitsverlust durch die RDP Session war nicht spürbar. Man konnte sich von Zuhause aus ganz bequem auf seinem Arbeitsplatzrechner ohne irgendwelche Einschränkungen im HMWK bewegen.

Das einzige Problem war, dass es keine Möglichkeit gab, den Rechner wieder herunterzufahren. Dies habe ich mit einer kleinen Batch-Datei gelöst die wie folgt aussieht:

shutdown -s -f -t 30 -c "Der Rechner wird nun ausgeschaltet."

-s = Fährt den Computer herunter.

-f = Erzwingt das Schließen ausgeführter Anwendungen ohne Vorwarnung.

-t = Legt die Zeitüberschreitungsperiode vor dem Herunterfahren fest.

-c = Kommentar bezüglich des Herunterfahrens

Nachträglich wurde mir allerdings von Giritech mitgeteilt, dass dieses Problem per Policy gelöst werden kann. Dies kann ich bestätigen.

6.7 Risikoanalyse

Eine Risikoanalyse ist die Aussage über Eintrittswahrscheinlichkeit und Schadensausmaß möglicher Risiken. Hierfür wurde für den Betrieb zur Veranschaulichung ein Risikograph erstellt.

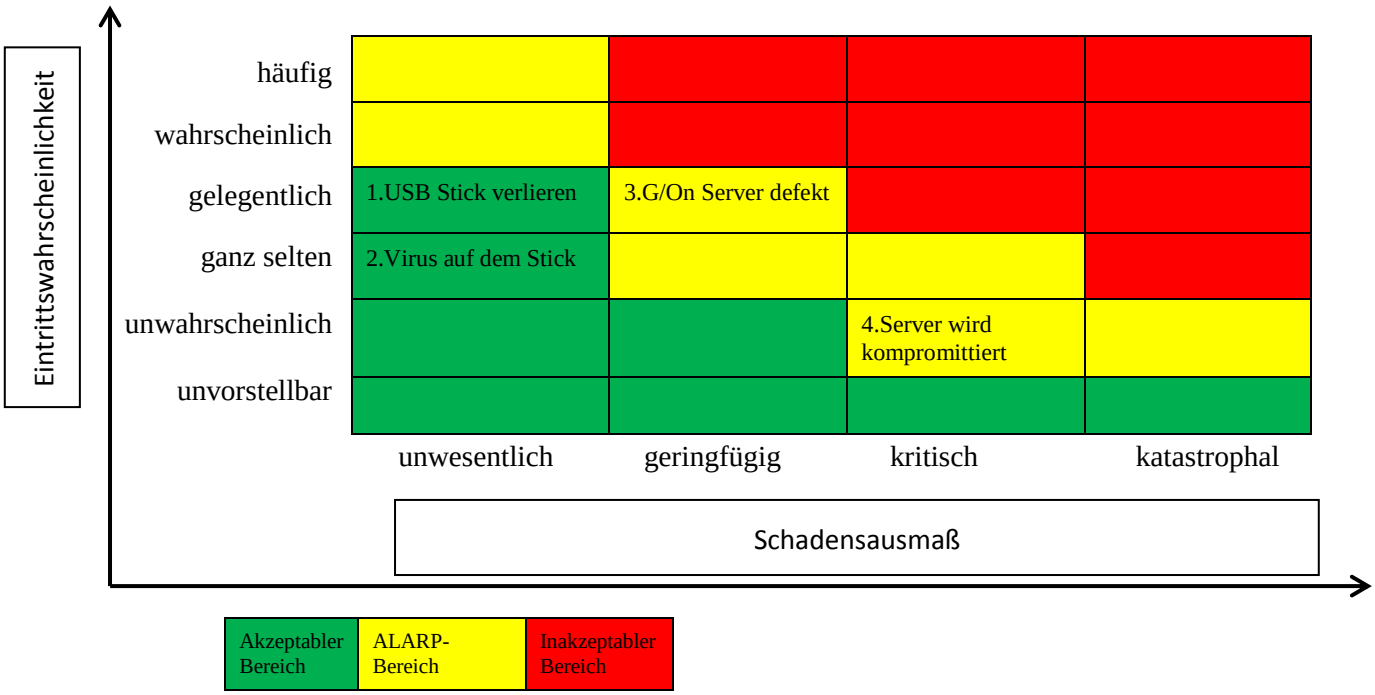


Abb. 09: Risikoanalyse

ALARP = As Low As Reasonably Practicable (so niedrig, wie vernünftigerweise praktikabel).

1. Gelegentlich kann der G/On USB-Token verloren gehen. Das ist allerdings nicht weiter tragisch, da jeder G/On USB-Token am Server gesperrt werden kann. Als zusätzliche Hürde, muss für den Unbefugten Benutzername und Kennwort bekannt sein.
2. Auf dem Wechseldatenträger ist ein Open Source Produk mit den Namen „Clamp Win“ installiert. Das Programm führt einen Virenscan durch, nachdem der Stick eingesteckt wird. Zusätzlich muss der Virus sich der über den lokalen PC / Laptop einen Weg durch die DMZ (Firewall → G/On Server →Router) finden, um ins Hausnetz zu gelangen.
3. Sollte der G/On Server defekt sein, kann ein neuer Server aufgesetzt und der G/On Installations Ordner per „Copy Paste“ dort eingefügt werden. Alle Einstellungen und Konfigurationen bleiben erhalten: „Cold Standby“.
4. Es ist eher unwahrscheinlich, dass der Server kompromittiert bzw., dass der Unbefugte sich Zugriff zum Hausnetz verschafft. Man müsste durch die DMZ (Firewall → G/On Server → Router) um Zugriff zu erlangen.

Ergänzend zu der Risikoanalyse muss darüber hinaus in Risikotypen unterschieden werden:

a) Die Lösung kann generell zu einem Unternehmensrisiko werden
   - missbräuchliche, unternehmensschädliche Nutzung
   - ungesicherte Öffnung des Unternehmens nach außen
   - damit verbunden "Intrusion risc", "man in the middle attack", "Session hitchhiking"

   Hier deckt G/On mit Ausnahme des menschlichen Faktors (leichtfertiger oder bewusster Missbrauch), durch sein mehrstufiges Sicherheitskonzept und seine Arbeitsweise alle Risiken ab.

b) Der Ausfall der Lösung stellt ein wirtschaftliches Risiko dar. Wenn Abläufe und Prozesse dezentralisiert bzw. mobil angeboten werden, ist eine hohe Verfügbarkeit elementar. Je mehr Komponenten und Instanzen zusammenwirken, desto aufwändiger gestaltet sich im Fehlerfall die Wiederherstellung.

   Hier kann G/On als "Single Point of Administration" bzw. "Single Point of Failure" auch dieses Risiko stark minimieren.

   - Cold Standby - Wiederanlauf eines Systems innerhalb weniger als zwei Stunden
   - Verkürzung dieser Zeit durch Einsatz virtualisierter Servertechnik (Image Rückspielung)
   - Failover durch redundante und lastverteilte wirksame Installation

6.8 Übergabe der Projektergebnisse

Die erzielten Projektergebnisse wurden in einem Meeting dem Projektverantwortlichen sowie dem gesamten IT-Team vorgestellt. Hierbei wurden Erkenntnisse, Probleme und deren Lösung, die während der Durchführung des Projekts erstanden sind, nochmals angesprochen und diskutiert.

Die komplette Übergabe erfolgte mit einer kleinen Schulung, da die IT-Mitarbeiter für die Nachbetreuung verantwortlich sind. Im Anschluss wurde auf das von mir erstellte G/On Installationsvideo und die Kundendokumentation hingewiesen.

7 Projektergebnis

7.1 Soll-Ist-Vergleich

Ein quantitativer Vergleich der geleisteten Stunden laut Projektantrag und der tatsächlich geleisteten Arbeitsstunden sind nachfolgend aufgeführt.

Soll-Ist Vergleich		
Projektteilschritt	Soll	Ist
Planung und Vorbereitung:		
1. Analyse des Ist – Zustandes	2,0 h	2,0 h
2. Soll-Konzeption definieren	2,0 h	2,0 h
3.Angebot einholen und Beschaffung	1,5 h	1,5 h
4. Planung der Umsetzung in die IT-Infrastruktur	2,5 h	1,5 h
Durchführungsplanung bzw. Realisierung:		
5. Aufbau und Installation der Hardware, Software-Komponenten	5,0 h	4,0 h
6. Konfiguration, Einrichtung und erste Funktionstests	3,0 h	5,0 h
7. Integration der Umsetzung in den Betriebsablauf	4,0 h	4,0 h
8. Erstellen der Benutzerdokumentation	2,5 h	1,5 h
Übergabe:		
9. Schulung der Mitarbeiter	2,5 h	1,5 h
10. Projektdokumentation	10,0 h	12,0 h
Gesamtstunden	**35,0 h**	**35,0 h**

Abb. 10: Soll-Ist Vergleich

7.2 Abweichungen

Zunächst war geplant, das Projekt für alle Mitarbeiter des Hauses zu realisieren. Im Laufe des Projektes stellte sich aber heraus, dass ein Terminal-Server wirtschaftlich besser in unseren Betriebsablauf passt. Da allerdings das Projekt mit 35 Stunden vorgegeben ist, würde die Integration eines Terminal Servers zu viel Zeit beanspruchen. Deshalb wird das Verfahren per Wake on LAN und sichere Remote Desktop Verbindung zunächst ausschließlich nur für die Administratoren der IT zur Verfügung gestellt. Das Wake on LAN Verfahren hat für Administratoren den Vorteil, dass Administrationssoftware wie Backup, Netzwerk-Assistenten etc. nicht auf einem Terminal-Server installiert werden muss. Außerdem können am Wochenende bequem Updates eingespielt werden. Das Terminal Server Verfahren wird nach dem Projekt in unsere IT-Infrastruktur übernommen.

8 Fazit

Meiner Meinung nach gibt es kein Projekt, das auf Anhieb funktioniert. Gerade in der IT kann die Analyse und Behebung eines Fehlers mehrere Tage benötigen. Auch in meinem Projekt gab es hin und wieder Komplikationen. Deshalb hat mich folgende Grafik sehr angesprochen, da ich den Frosch gut verstehen kann.

Quelle: http://www.hofheimnet.de/never_ever_give_up.jpg

Abb. 11: Fazit

So gab es beispielsweise bei der Installation und Konfiguration des Servers weniger Probleme. Allerdings mussten am Client Rechner einige Einstellung vorgenommen werden. Zum Beispiel musste ich die lokale Richtlinie an jedem einzelnen Rechner so bearbeiten, dass jeder Benutzer die Befugnis bekommt, den Rechner Remote ausschalten zu dürfen. Zum anderen war die Wake on LAN-Konfiguration für jeden Rechner anders. In Zukunft werde ich mir vorher überlegen, welche Probleme auftauchen könnten, um diese dann im Vorfeld schneller beheben zu können.

Die Giritech Anleitungen waren größtenteils in englischer Sprache verfasst. Hier konnte ich meine Englischkenntnisse unter Beweis stellen. Dabei ist mir aufgefallen, dass mir viele Vokabeln nicht mehr geläufig waren. Daher plane ich als Weiterbildung einen Kurs, in dem ich mein technisches Englisch auffrischen kann.

Der Umgang mit so einer umfangreichen Projektdokumentation ging mir nicht so leicht von der Hand, wie ich anfangs eigentlich gedacht hatte. Hier werde ich beim nächsten Mal, was Formatierungen und Tabellen angeht den Zeitpuffer erhöhen.

Die stets kompetenten Mitarbeiter der Firma Giritech standen mir bei allen technischen Problemen zur Verfügung und es gab keine Frage die nicht beantwortet werden konnte.

Ich habe sehr viel in dem Projekt über mich lernen können und konnte mir gleichzeitig auch neues Wissen aneignen.

Literaturverzeichnis

G/On – der richtige Access ist entscheidend - Broschüre

Giritech [2010]

G/On Setup und Konfiguration

http://www.giritech.de/downloads/software/gon5/gon_getting_started_setup_and_configuration.pdf

Stand: 14.03.2011

G/On Management Info

http://www.giritech.de/downloads/software/gon5/gon_getting_started_management.pdf

Stand:14.03.2011

G/On 5 Produktankündigung

http://www.giritech.de/downloads/software/gon-5/Produktankuendigung-Version-54.pdf

Stand: 14.03.2011

G/On vs VPN

http://www.giritech.de/downloads/pdf/Technologie-Vergleich-GOn-VPN.pdf

Stand: 14.03.2011

Abkürzungsverzeichnis

AD	Active Directory
CAT-6	Kategorie 6
DMZ	Demilitarisierte Zone
DV-OrgB	Datenverarbeitung organisatorischer Bereich
HeDOK	Hessische Dokumenten Verwaltung
HMWK	Hessisches Ministerium für Wissenschaft und Kunst
HRZ	Hochschulrechenzentrum
HZD	Hessische Zentrale für Datenverarbeitung
IT	Informationstechnik
LWL	Lichtwellenleiter
MANDA	Metropolitan Area Network Darmstadt
MB	Megabyte
MBit	Megabit
MwSt.	Mehrwertsteuer
PC	Personalcomputer
TUD	Technische Universität Darmstadt
VPN	Virtuelles Privates Netzwerk

Abbildungsverzeichnis

Abb. 01: Personalplanung. 3
Abb. 02: Sachmittelplanung 3
Abb. 03: VPN – Kosten 4
Abb. 04: G/On – Kosten 4
Abb. 05: G/On / VPN – Kosten 5
Abb. 06: G/On – VPN Kosten Unterschied 5 User/10 Jahre 5
Abb. 07: Ablaufplan 6
Abb. 08: Funktionstest – G/On Zugang 9
Abb. 09: Risikoanalyse 10
Abb. 10: Soll-Ist Vergleich 12
Abb. 11: Fazit 13

Anhang

- Kundendokumentation
- Administrationshinweise
- Bildergalerie
- G/On Configuration / Management
- G/On täglich im Einsatz
- G/On vs. VPN

Hessisches Ministerium
für Wissenschaft und Kunst

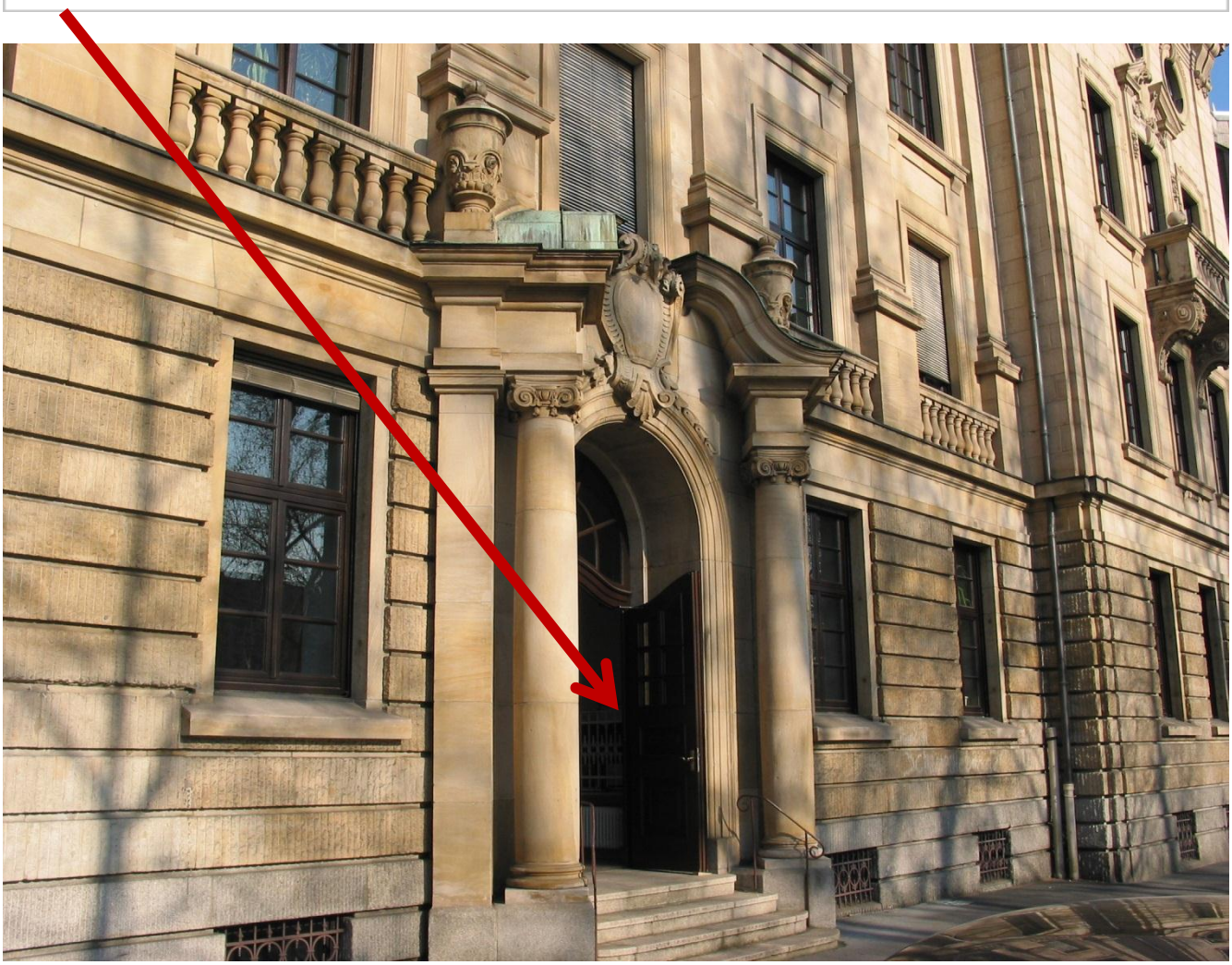
HESSEN

Kundendokumentation

Aufbau einer einfachen und sicheren Remoteverbindung ins HMWK mit G/On

G/On™ Mobiler Remote Access ohne VPN-Strukturen

GIRITECH®

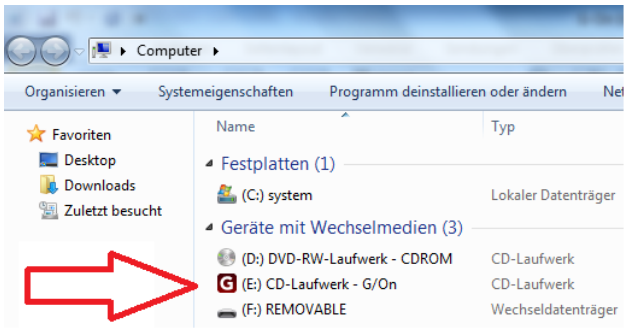


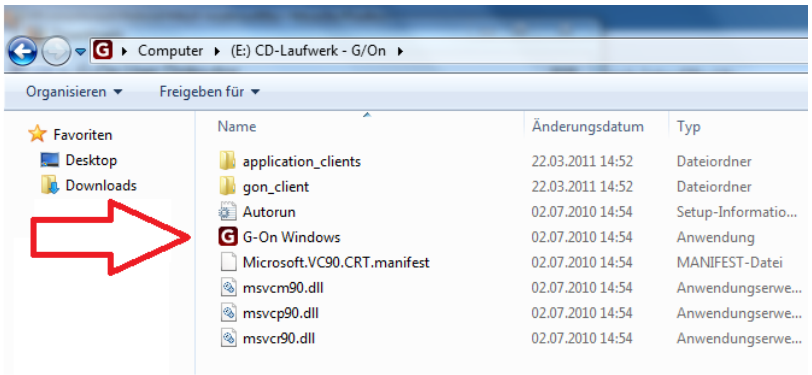
M. Axtmann

1. Stecken Sie den G/On USB Stick in den USB Steckplatz an Ihrem Rechner

2. Es öffnet sich ein Fenster. Falls nicht, ist der *Autostart* wahrscheinlich deaktiviert. Gehen Sie bitte in diesem Fall wie folgt vor:

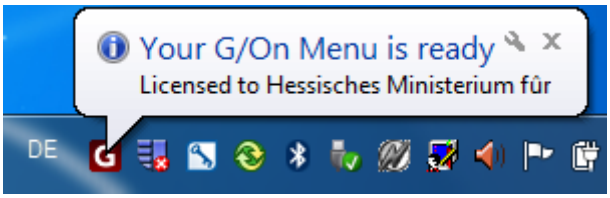
   - Arbeitsplatz öffnen
   - CD-Laufwerk G/On öffnen
   - G/On Windows.exe ausführen





3. Es öffnet sich ein neues Fenster. Hier geben Sie Ihre gewohnten Windows-Anmeldedaten aus dem HMWK ein.

4. Nach erfolgreicher Authentifizierung der Daten erscheint rechts unten in der Taskleiste folgendes Symbol:



5. Klicken Sie auf das G/On Symbol und wählen dann *Arbeitsplatz einschalten*. Der Rechner wird nun im HMWK hochgefahren.

   Warten Sie ca. 3 Minuten um sicher zu gehen, dass der Rechner auch komplett hochgefahren ist. Anschließend klicken Sie auf *Arbeitsplatz verwenden*.

   Der Rechner baut eine Remote-Verbindung auf und Sie können wie gewohnt an Ihrem HMWK Rechner arbeiten.

6. Um den Rechner im HMWK wieder auszuschalten, klicken Sie die Verknüpfung „G-On, Shutdown“ per Doppelklick an. Der Rechner wird dann nach 30 Sekunden ausgeschaltet.

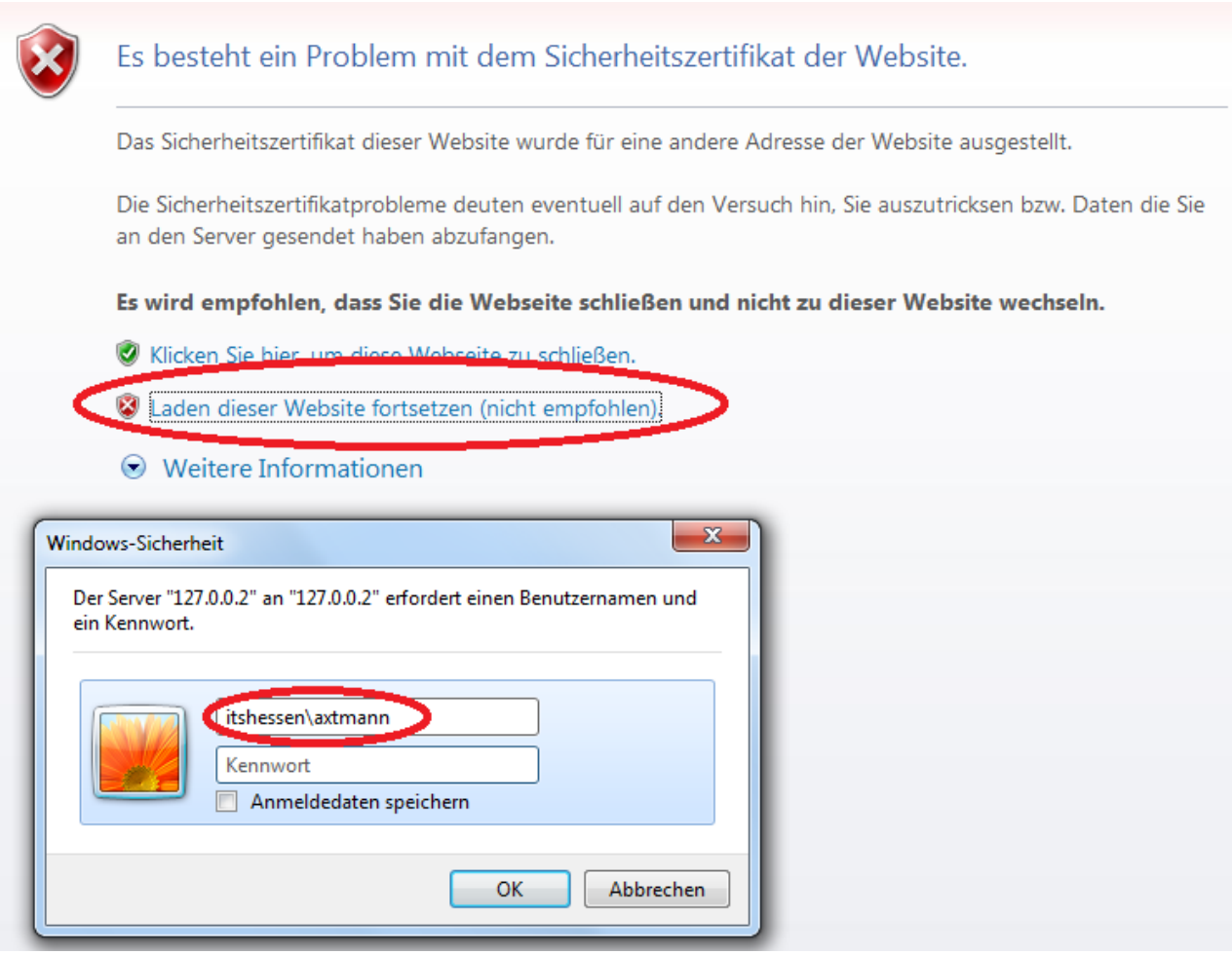
Hessisches Ministerium
für Wissenschaft und Kunst

HESSEN

Zugang zum Outlook Web-Access

Wenn Sie nur E-Mails lesen möchten ohne den Rechner hochzufahren, können Sie dies über den Outlook Web Access tun. Navigieren Sie im G/On Menü zu:

„Alle Programme -> Zugang zum Outlook Web Access“



M. Axtmann

FAQ - Fehlermeldungen und Lösungen

Wie kann ich die Remoteverbindung minimieren/schließen?

- Navigieren Sie mit der Maus zum oberen Bildschirmrand um die Remote Verbindung zu minimieren oder zu schließen.

Ich habe den G/On Stick eingesteckt und die „G/On Windows.exe“ gestartet. Danach passiert allerdings nichts mehr.

- Der G/On Client kann keine Verbindung zum G/On Server herstellen. Bitte überprüfen Sie Ihre Internet Verbindung.

Ich bekomme beim Anmelden die Fehlermeldung: „Insufficient Autorisation“.

- Vermutlich haben Sie sich vertippt. Bitte überprüfen Sie nochmals Benutzername und Passwort. Die IT kann ihr Passwort im Notfall zurücksetzen.

Nach einem Klick auf „Arbeitsplatz verwenden“ meldet mir G/On: „Portforward Error: Server unable to connect.“

- Der Rechner im HMWK scheint nicht hochgefahren zu sein. Haben Sie vielleicht die Steckdosenleiste ausgeschaltet? Melden Sie sich bei der IT, damit die Konfiguration am Rechner nochmals überprüft wird.

Administrationshinweise

Falls der G/On Server neuinstalliert/konfiguriert werden muss, so schauen Sie bitte das Video an, das ich während der Installation/Konfiguration erstellt habe.

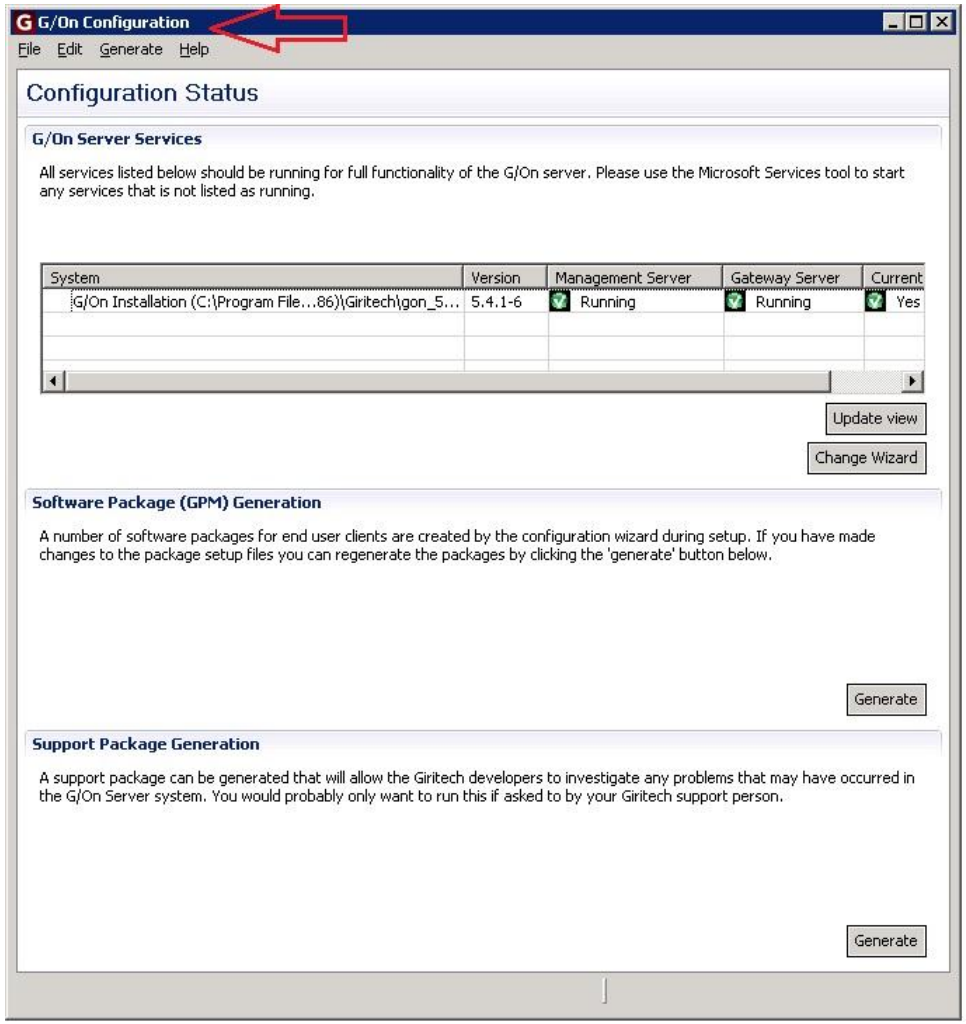
Es ist zu finden unter:
\\srvhmwkfil0002\hmwk\IT\G-On\Installation_Konfiguration.avi

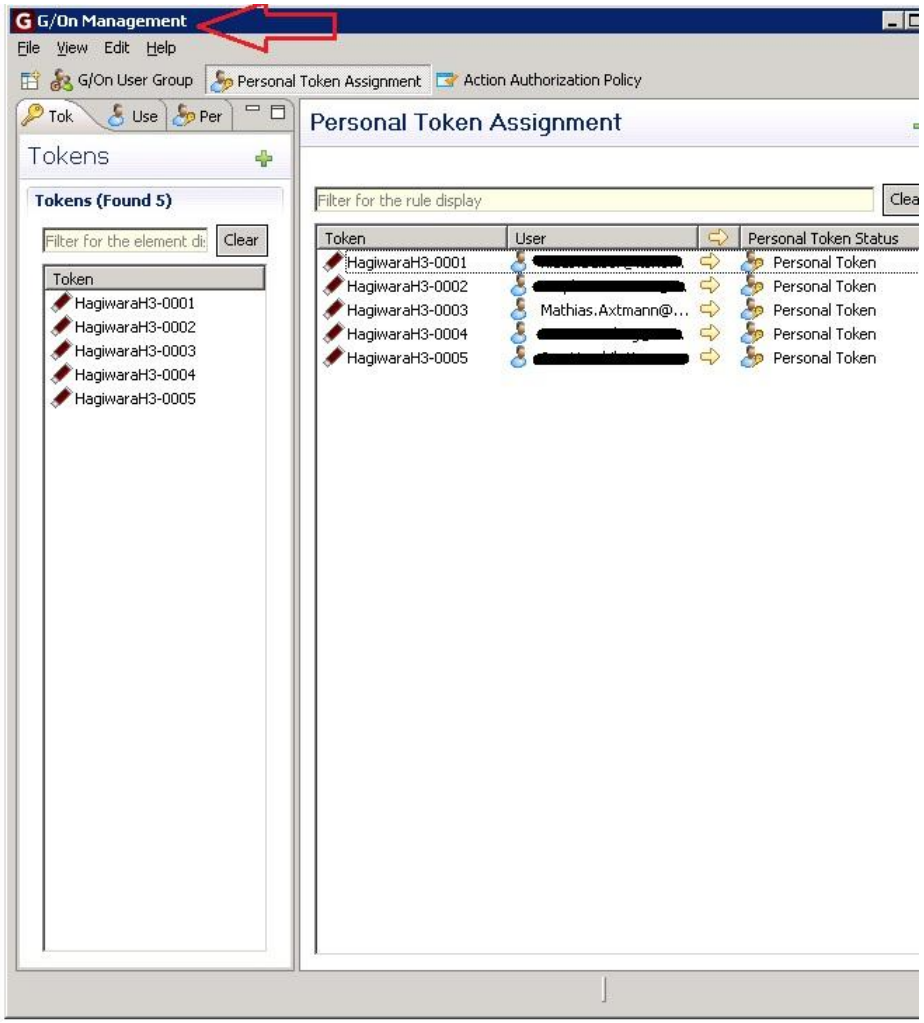
Bildergalerie

G/On Server

G/On USB-Token

G/On Configuration / Management





Quelle: www.giritech.com

Technologievergleich

G/On versus VPN

Diese Übersicht zeigt die Unterschiede zwischen G/On sowie den beiden etablierten VPN Technologien auf. Bitte beachten Sie, dass der Vergleich eines konkreten Produkts mit zwei Technologien nicht sämtliche besonderen Merkmale spezifischer VPNs abbilden kann. Umfassende Informationen zur einzigartigen Technologie von G/On finden Sie auf www.giritech.de.

	IPSec VPN	SSL VPN	Giritech G/On
erforderliche User-Rechte			
zur Installation	Admin	User + Rechte für Plugins	Gast
zur Ausführung	User	User	Gast
Authentifizierung			
Hardware-Authentifizierung	Drittanbieter	Drittanbieter	integriert
Benutzer-Authentifizierung	Ja	Ja	Ja
"Trusted" PC erforderlich	Ja	Nein, aber empfehlenswert für Plugins & Cache	Nein
Gegenseitige Client/Server Authentifizierung zur Vorbeugung von Phishing	Ja, Verwendung eines “pre-shared secrets“	Ja, über Zertifikate	Ja, echte gegenseitige C/S Authentifizierung
Zugriffssicherheit			
Autorisierung	Drittanbieter	Drittanbieter	integriert
Sicherheitszonen	Nein	Nein	Ja
Active Directory Anbindung	herstellerspezifisch	herstellerspezifisch	integriert, optional
Lokale Benutzerverwaltung	herstellerspezifisch	herstellerspezifisch	integriert
verwertbare Endpunkt-Informationen (Daten im Cache, z. B. Passworte)	Ja	Ja	Nein
Daten-Verschlüsselung	max. 256 bit AES mit statischen Keys	SSL (typisch 128-bit AES, max. 256-bit AES mit statischen Keys)	256 bit AES + wechselnde Keys während der Session, 163 bit ECC während Aufbau
Schutz vor "man-in-the-middle" Angriffen und Replay-Attacken	Ja wenn das "pre-shared secret" ausreichend geschützt ist	Ja, wenn Zertifikat ausreichend geschützt ist	Ja, durch Prüfsummen und Zeitstempel, die jedem Paket angefügt sind
verwendete Tunneling-Protokolle	L2TP, P2PP und andere je nach Hersteller	L2TP, P2PP und andere je nach Hersteller	keine
Absicherung der Endpunkte			
Antivirus	erforderlich	erforderlich	empfohlen
Firewall	erforderlich	erforderlich	empfohlen
Client-Filterung	MAC/IP-Adresse	MAC/IP-Adresse	Hardware EDC Nummer und weitere Informationen
unerwünschte Prozesse, Malware-Prozesskontrolle	Drittanbieter	Drittanbieter	integriert, “lock to process”
Verteidigung gegen Angreifer	DMZ oder Applikationsserver	DMZ oder Applikationsserver	direkt auf der Client-Seite ausserhalb des Unternehmens
Zugriffsebene			
Art des Zugriffs	Netzwerkebene	Applikationsebene	Applikationsebene
Mitglied im Netzwerk	Ja	abhängig vom Produkt und Setup	Nodeless-Client, PC ist kein Mitglied im Netzwerk und besitzt keine IP im LAN
Sonstiges			
Offene Ports	mehrere	mehrere	einer
Administration und Verwaltung	dezentral unter Verwendung von Tools und Browser, zusätzlich Verwaltung der Drittanbieterprodukte und Sicherheitsapplikationen	dezentral unter Verwendung von Tools und Browser, zusätzlich Verwaltung der Drittanbieterprodukte und Sicherheitsapplikationen	vollständig zentralisierte Verwaltung ausschliesslich über den G/On Server, (Deployment, Token-Verwaltung, Zugriffsmanagement, Logging, Auditing uvm.)
Infrastruktur	typischerweise 2 bis 4 verschiedene Hersteller	typischerweise 2 bis 4 verschiedene Hersteller	1 einziges Produkt (“all-in-one” end-to-end Lösung)

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech’s core intellectual property includes the patent-pending systems and methods called EMCADS™. Die Informationen in diesem Dokument geben ausschliesslich den Kenntnisstand zum Zeitpunkt der Veröffentlichung wieder. Sie wurden sorgfältig recherchiert und zusammengestellt. Wir weisen dennoch ausdrücklich darauf hin, dass die gegeben Informationen aufgrund nicht regelmässiger Aktualisierungen oder Änderungen nicht mehr aktuell sein können. Sämtliche Informationen beinhalten keine Zusicherungen oder Gewährleistungen, auch übernehmen wir keine Haftung für mögliche Schäden, die aufgrund der Nutzung der Informationen entstehen können. Bei Unstimmigkeiten, die aufgrund der Übersetzung möglich sind, gelten die Sprachregelungen der dänischen Dokumente. Alle genannten Handelsbezeichnungen/Produktnamen sind Dienstmarke, Marke oder eingetragene Marke des jeweiligen Inhabers oder Herstellers. Copyright © Giritech GmbH Juli 2008.