Beispiel IT AUDIT REPORT

IT Risiko Analyse für KMUs

Max Mustermann GmbH
Landstraße 1
A-4020 Linz

Version: 0.1
Stand: 31. Oktober 2010
Klassifizierungsstatus: Vertraulich

data security management
data management gmbh
auf der halde 27
a-4060 leonding
0732 791100 - fax dw 25
info@datasec.at

Versionshistorie Dokument:

Version	Anmerkung	Datum	Bearbeiter
0.1	Initial Draft	29. Oktober 2009	Andreas Wagner, MSc.

Auditablauf:

Datum	Auditor	Beteiligte
20. Oktober 2009	DI Heinz Platzer	DI Peter Max Fr. Maier

Der nachfolgende Report fasst die Ergebnisse der Befragung zusammen, welche im Zuge der „IT Risiko Analyse für KMUs“ gemacht wurden.

Die im Folgenden angeführten Punkte wurden in Übereinstimmung mit dem derzeitigen Stand der Technik nach bestem Wissen und Gewissen ausgearbeitet und erläutert.

Die „IT Risiko Analyse für KMUs“ baut primär auf den Antworten der Befragten auf. Eine genaue technische Analyse ist nicht Inhalt dieses Audits. Diese weiterführende Maßnahme kann gesondert durchgeführt werden.

Der vorliegende Auditbericht darf nur nach Zustimmung der zuständigen, verantwortlichen Parteien des Kunden weitergegeben werden.

Die Struktur und Aufbau des Reports bzw. des Audits und dessen Ablaufes ist geistiges Eigentum der Firma Data Management GmbH und darf nicht ohne vorherige schriftliche Zustimmung für eigene Zwecke oder jener Dritter verwendet werden.

data security management
data management gmbh
auf der halde 27 0732 791100 - fax dw 25
a-4060 leonding info@datasec.at

Inhaltsverzeichnis

Major Findings – wichtigsten Maßnahmen 4

Minor Findings – weiterführende Maßnahmen 5

Allgemeine Unternehmens – IT 7

Backup der Daten 8

Mitarbeiter 9

Rollen und Verantwortlichkeiten 10

Dokumentation 11

Schutz der Daten / Zugriff 12

Aufbau und Wartung zentraler Services 13

Physikalischer Schutz 14

Netzwerkverbindungen 15

Internet / Intranet 16

Updates / Sicherheitslücken 17

Schutz vor Malware 18

Conclusio 19

data security management
data management gmbh
auf der halde 27
a-4060 leonding
0732 791100 - fax dw 25
info@datasec.at

Major Findings – wichtigsten Maßnahmen

(Die Details zu den Major Findings sind auf den jeweiligen Seiten **fett markiert**)

<< 1.ma >> Besprechung von realistischen Worst Case Szenarien mit Betreuer
(Seite 7)

<< 2.ma >> Consulting durch unabhängige Stelle – externe Berater
(Seite 7)

<< 3.ma >> Fixierung bzw. schriftliche Festlegung der IT (Sicherheits-) Richtlinien und firmenweite Kommunikation
(Seite 9)

<< 4.ma >> Konkrete, bewusstseinsbildungen Maßnahmen für Mitarbeiter – Schulungen
(Seite 9)

<< 5.ma >> Aktuelle Liste der wichtigsten Ansprechpartner in Printform
(Seite 10)

<< 6.ma >> Betreuung der Ausschreibungssoftware XYZ seitens eines Herstellers - Support durch Einzelperson
(Seite 10)

<< 7.ma >> Technische Evaluation des IST Zustandes der IT Infrastruktur hinsichtlich Schwachstellen
(Seite 17)

data security management
data management gmbh
auf der halde 27
a-4060 leonding
0732 791100 - fax dw 25
info@datasec.at

Minor Findings – weiterführende Maßnahmen

(Die Details zu den Minor Findings sind auf den jeweiligen Seiten unterstrichen)

<< 1.mi >> Automatische Sperrung der Workstations
(Seite 9)

<< 2.mi >> Vertretung von Fr. Maier – schriftlich hinterlegte Informationen zu Arbeitsabläufen auf Netzwerkshare
(Seite 10)

<< 3.mi >> Sichere Hinterlegung aktueller Passwörter und Zugangsdaten für IT Systeme
(Seite 11)

<< 4.mi >> Passwörter von Mitarbeiter werden mittles nachvollziehbarem Schema erstellt
(Seite 12)

<< 5.mi >> Für externe Projektmitarbeiter werden simple Passwörter definiert
(Seite 12)

<< 6.mi >> Schriftliche Dokumentation des Workflows für bzw. von externen Projektmitarbeitern
(Seite 12)

<< 7.mi >> Automatisierte Überwachung wichtiger Systemwerte
(Seite 13)

<< 8.mi >> Aufbau und Standort von Hardware und Komponenten im Technikraum
(Seite 13)

<< 9.mi >> Regelmäßige Reinigung der Server und wichtiger Komponenten
(Seite 13)

<< 10.mi >> Einbindung der Server hinsichtlich längerem Stromausfalles bez. USV
(Seite 13)

<< 11.mi >> Umweltbedingten Meldeanlagen im Technikraum
(Seite 14)

<< 12.mi >> Entsorgung alter Datenträger
(Seite 14)

<< 13.mi >> Einheitliche Konfiguration der Windows Client Firewall
(Seite 15)

data security management
data management gmbh
auf der halde 27
a-4060 leonding
0732 791100 - fax dw 25
info@datasec.at

<< 14.mi >> Einsatz von Web-Content Filtern
(Seite 16)

<< 15.mi >> Effizienz des Spam-Filters
(Seite 16)

<< 16.mi >> VPN Verb. ins interne System teilweise von potentiell unsicheren Systemen
(Seite 16)

<< 17.mi >> Befürchtete Gefahr von verlorenen Emails bei Störung der Internetleitung
(Seite 16)

<< 18.mi >> Unklarheit des externen Zugriffs auf Telefonanlage
(Seite 16)

<< 19.mi >> Überprüfung auf bestehende Sicherheitslücken von installierten Anwendungen bzw. Software auf Workstations / Servern
(Seite 17)

data security management
data management gmbh
auf der halde 27
a-4060 leonding
0732 791100 - fax dw 25
info@datasec.at

Allgemeine Unternehmens – IT

Es gibt folgende Unternehmensbereiche:

- Sekretariat
- Buchhaltung
- Planerstellung
- 4 ARGEn welche extra bilanziert werden

Für die Bereiche werden folgende Services bereitgestellt:

Grundsätzlich 3 Server:
- Exchange (Email, Kalender)
- Fileserver (Projektdateien)
- FTP Server für Datenaustausch mit Projektbeteiligten
- Transfer Laufwerke für ARGEn (Eingehende VPN Verbindungen)
- SPS für Projektbeteiligte (Read-Only der per SPS bereitgestellten Dateien)

Telefonie über einfache Telefonanlage, xDSL Internet, Mobiltelefone, PDA, Mobiles Internet mittels 2x A1 Datenkarten

Die Abhängigkeit der Abteilung zu den IT Services wird von den Geschäftsführern als sehr hoch eingeschätzt: „Ohne EDV sperren wir zu“
Maximal 1 Tag kann mit alternativen Aufgaben überbrückt werden.

Am wichtigsten ist hierbei die Verfügbarkeit der Projektdateien und Emails, da das meiste nur digital abgelegt ist.
<< 1.ma >> Es ist zwar eine tägliche Sicherung vorhanden, für den Worst Case müsste geklärt werden, wie rasch der IT Betreuer die Sicherungsbänder temporär auf ein Backupsystem bereitstellen kann.
Konkrete Notfallpläne für diverse Szenarien wurden bisher weder praktisch noch theoretisch durchgespielt. (Grobe Ablaufplanung…)

Die Verantwortlichkeit für die IT trägt die Geschäftsführung bzw. der jeweilige Projektleiter. Regulatorische oder vom Gesetzgeber festgelegte Richtlinien hinsichtlich des Umgangs mit IT und Daten des Unternehmens sind nicht im Detail bekannt.

Informationssicherheit nimmt im Unternehmen derzeit einen als „mittel“ genannten Stellenwert ein.

Die Vertraulichkeit der Projektdaten ist eher unwichtig, solange die Daten für die Mitarbeiter unverfälscht zur Verfügung stehen.

<< 2.ma >> Es gibt keine derzeit „Gewaltentrennung“ hinsichtlich der bestehenden IT Infrastruktur bzw. keine externe beratende Instanz im Hintergrund welche bei Bedarf zusätzlich konsultiert wird.

data security management
data management gmbh
auf der halde 27 0732 791100 - fax dw 25
a-4060 leonding info@datasec.at

Backup der Daten

Gesichert wird täglich von Montag bis Freitag.
Inhalt der Sicherung ist immer die Konfiguration bzw. wo nötig das gesamte Betriebssystem der Server, die Daten sowie auch regelmäßig alte Projekte. Es erfolgt jeden Tag eine Vollsicherung mit derzeit ca. 350 GB Daten.

Die Backupbänder werden im Safe im Serverraum gelagert. Der Zugriff darauf ist nur mittels Schlüssel möglich -> Fr. Maier bzw. Ersatzschlüssel -> Zugriff Geschäftsleitung

Das tägliche Backup wird von Frau Maier überwacht, die Geschäftsführer wissen über das grundsätzliche Backup-Prozedere Bescheid. Die Backupsoftware schickt nach jeder Sicherung ein Email über den Status der Sicherung an Fr. Maier bzw. an die Geschäftsleitung.

Die Backupsoftware überprüft nach erfolgter Sicherung ob die Daten richtig auf das Backupmedium geschrieben wurden. (Integritätscheck)

Die Wiederherstellung einzelner Daten bzw. Projekte kann von Fr. Maier durchgeführt werden. Größere Wiederherstellungen müssen vom IT Betreuer durchgeführt werden.

Wichtige Konfigurationsdateien von z.B. der Firewall werden regelmäßig gesichert.

Gesetzliche Archivierungsvorschriften werden erfüllt.

Wichtige Daten werden nur auf den Servern gespeichert wo diese auch gesichert werden - nicht auf Wechseldatenträgern oder auf beispielsweise C:\

data security management
data management gmbh
auf der halde 27
a-4060 leonding
0732 791100 - fax dw 25
info@datasec.at

Mitarbeiter

Es gibt Handbücher welche betriebsinterne Vereinbarungen und Anweisungen bezüglich Firmenautos, Projektanlage, Emailsignaturen etc. beinhalten. Die vorhandenen Handbücher werden von Fr. Maier bei Bedarf aktualisiert.

<< 3.ma >> Policies bzw. Sicherheitsrichtlinien für den richtigen bzw. erlaubten Umgang der Betriebs-IT sind nicht schriftlich fixiert. Diese werden aber mündlich kommuniziert, soweit daran gedacht wird.

Neue Mitarbeiter werden auf die Systeme entsprechend eingeschult und bekommen so den gewünschten Umgang mit der Unternehmens-IT erklärt.
<< 4.ma >> Es gibt keine expliziten bewußtseinsbildenden Maßnahmen bzw. Schulungen zum Thema Informationssicherheit, welche das allgemeine Sicherheitsniveau stark anheben würden. (Informationen über Social Engineering etc.)

Sensible Bereiche bezüglich der IT bzw. Daten sind weitgehend definiert, es ist bekannt welche Mitarbeiter bzw. Externe darauf Zugriff haben.

Die Mitarbeiter haben teilweise lokal Adminrechte, allerdings nur falls diese wirklich benötigt werden bzw. wenn der jeweilige Mitarbeiter als „vertrauenswürdig genug“ (langjähriger MA) eingestuft wurde.

Falls ein MA die IT unsachgemäß bzw. in unerlaubter Weise benutzt werden über direkte Gespräche die Probleme angesprochen – das hat sich bewährt. Keine konkreten Konsequenzen definiert, situationsabhängig.

Durch die Mitarbeiterbesprechungen entwickelt sich im Team eine Eigendynamik in der gegenseitige Kontrolle ermöglicht wird.

Die Corporate Identity wird als sehr wichtig erachtet, Dokumente sind entsprechend der Vorgaben der Handbücher von den Mitarbeitern zu erstellen. Die firmenweite CI wird von den Mitarbeitern entsprechend genutzt.

Es gibt die mündliche Anweisung seinen Arbeitsplatz vor Abwesenheit aufzuräumen bzw. vertrauliche Unterlagen entsprechend zu verstauen (Clear Desk).

<u><< 1.mi >> Der Bildschirm wird auch nach längerer Abwesenheit des Users nicht automatisch gesperrt. Die User richten sich diese Option je nach Bedarf selbst ein.</u>

data security management
data management gmbh
auf der halde 27 0732 791100 - fax dw 25
a-4060 leonding info@datasec.at

Rollen und Verantwortlichkeiten

Eine aktuelle Liste mit den Ansprechpartnern (Hardware, Software, Dienstleistern) wird im Outlook unter den Kontakten geführt. Die Inhalte von Outlook werden offline gecached. Zugriff also auch nach Ausfall von Exchange möglich.
<< 5.ma >>Es gibt keine für jeden bekannte und zugängliche aktuelle bzw. ausgedruckte Liste mit den wichtigsten Kontakten zu den jeweiligen Themen.

Interne Verantwortlichkeiten sind definiert und den Mitarbeitern bekannt. Für die interne IT ist Fr. Maier bzw. Fr. Buchner zuständig.

Die definierten Rollen werden eingehalten, es gibt für gewöhnlich kein „handeln auf eigene Faust“.

Bei den Geschäftsführern gibt es eine Vertreterregelung. Buchhaltung und Sekretariat haben großes gemeinsames Wissen. Die interne Betreuung der IT wird von Fr. Maier bzw. Fr. Hainberger durchgeführt.

Der externe IT Betreuer (Service GmbH) verfügt über genügend Kapazität und Wissensträger für die Betreuung der IT des Kunden.

<< 2.mi >> Die Aufgaben von Fr. Maier könnten auch von anderen Mitarbeitern zum größten Teil erledigt werden. Die Informationen wie bestimmte Arbeitsschritte zu erledigen sind stehen alle schriftlich hinterlegt am Netzwerkshare. Es ist allerdings unklar ob dies den Vertretern bzw. Mitarbeitern bekannt ist.

Der „Ausfall“ eines Mitglieds der Geschäftsführung führt naturgemäß zu Herausforderungen im normalen Tagesablauf.

<< 6.ma >> Hr. Berger betreut auf mündliche Zusage weiterhin die Ausschreibungssoftware XYZ, obwohl er nicht mehr zuständig ist (Wechsel zu Fa. Haidmann – direkte Konkurrenz). Er ist der einzige welcher sich professionell um die evtl. Probleme der Software kümmern kann. Die Software ist für die Ausschreibungen der Firma wichtig!

data security management
data management gmbh
auf der halde 27 0732 791100 - fax dw 25
a-4060 leonding info@datasec.at

Dokumentation

Ein schematischer Netzwerplan ist vorhanden und nach der letzten größeren Änderung auch aktuell. Detailliertere Dokumentationen liegen beim IT Betreuer auf.

Dokumentationen zu speziellen Softwareinstallationen bzw. Userlisten sind teilweise vorhanden.

Die eingesetzte Software ist entsprechend lizenziert, auf allen Workstations ist ziemlich die Gleiche Ausstattung an Programmen vorhanden. Alle Workstations sind nach einer grundsätzlich einheitlichen Baseline aufgesetzt. Es ist Office 2003 und 2007 im Einsatz (-> Verfügbarkeit von „alten“ Office Lizenzen bei Lieferanten)

Änderungen an der IT Infrastruktur werden vorab mit Fr. Maier abgesprochen.

Die implementierten bzw. vorgenommenen Schutzmaßnahmen sind laut Geschäftsleitung durch den IT Betreuer dokumentiert.

Zugangsdaten für verschiedenste Services (A1, Inode, WKO etc.) sind per Mail im Postfach von Fr. Maier gespeichert. Auf dieses Postfach hat auch die Geschäftsführung Zugriff. Einige dieser Zugangsdaten werden auch in einem Ordner im Büro abgelegt.
<< 3.mi >> Die aktuellen Passwörter und Zugänge der Systeme werden nirgends sicher hinterlegt, diese sind nur Fr. Maier und dem IT Betreuer bekannt.

Das angesprochene „Büchlein“ von Fr. Maier enthält keine sensitiven Informationen oder Zugangsdaten.

data security management
data management gmbh
auf der halde 27 0732 791100 - fax dw 25
a-4060 leonding info@datasec.at

Schutz der Daten / Zugriff

Jeder User hat einen eindeutigen Benutzeraccount.

Die lokale Anmeldung an den Workstations ist nicht möglich, es gibt lokal nur das Benutzerkonto „Administrator“.

Der Zugriff auf Daten bzw. Informationen ist generell nur über Zugangsdaten (Username + Passwort) möglich.

Die Geschäftsleitung, Fr. Mangold, Fr. Maier bzw. die Administratorkonten haben komplexe Passwörter mit hoher Sicherheit.
<< 4.mi >> Alle Mitarbeiter haben Passwörter nach einem für Kundige nachvollziehbaren Schema.

<< 5.mi >> Externe Projektmitarbeiter haben Passwörter welche laut Fr. Maier eher simpel aufgebaut sind. Diese werden von Fr. Maier fixiert, die externen User können diese Passwörter nicht ändern.

Grundsätzlich werden alle Arten von Wechseldatenträgern bei Bedarf verwendet. Es gibt keine Einschränkung oder Vorgabe welche besagt dass private Hardware nicht verwendet werden darf.

Als kritisch eingestufte Informationen und Daten werden durch NTFS Sicherheitseinstellungen besonders geschützt. Auf diese Bereiche haben nur Fr. Maier, Fr. Mangold sowie die Geschäftsleitung Zugriff. Auf sämtliche Projektdaten haben alle internen Mitarbeiter Vollzugriff. Einschränkungen und Ausnahmen gibt es teilweise für externe Projektmitarbeiter.

Laptops, Smartphones bzw. PDA’s werden nicht geschützt. Allerdings ist die Vertraulichkeit der Daten (Projekte etc.) oder Emails darauf weniger problematisch. Es ist „egal wenn diese Daten wer anderer kriegt“. Solange die Daten auf den Servern verfügbar sind ist das kein Problem.

Der IT Dienstleister sowie Fr. Maier haben Zugriff auf sämtliche Daten bzw. auf alle Systeme.

<< 6.mi>> Es existiert kein schriftlich fixierter Ablaufplan welcher die bestehenden Workflows für externe Projektmitarbeiter beschreibt (Transferlaufwerke, SharePointPortal Server, FTP…) Wissen darüber liegt im Detail bei Fr. Maier.

data security management
data management gmbh
auf der halde 27 0732 791100 - fax dw 25
a-4060 leonding info@datasec.at

Aufbau und Wartung zentraler Services

Durch die Installation des neuen Fileservers ist wieder ausreichend Kapazität vorhanden. Andere Engpässe hinsichtlich CPU, RAM etc. sind nicht bekannt bzw. sind diese derzeit nicht vorhanden.

<< 7.mi >> Die Überprüfung auf freien Speicherplatz und der Check einiger anderer wichtiger Systemwerte erfolgt regelmäßig manuell durch Fr. Maier.

Visuelle oder hörbare Alarme der Systeme werden durch Fr. Maier wahrgenommen und entsprechend bearbeitet bzw. weitergeleitet.

Einige zentrale Systeme schicken Statusemails an die Verantwortlichen.
<< 7.mi >> Es gibt aus Gründen des Aufwandes keine automatisierte 24/7 Überwachung der zentralen Server bzw. Services hinsichtlich wichtiger Umgebungswerte.

Die zentralen Systeme sind teilweise mit redundanten Bauteilen ausgestattet (Raid, Lüfter, Netzteile)

Die Verkabelung der Systeme ist zweckmäßig allerdings nicht sauber.
<< 8.mi >> Es gibt einen Serverschrank der allerdings seine Funktion wenig bis gar nicht erfüllt, die Server stehen verteilt im Technikraum. Mehrere Monitore stehen für den Zugriff auf die Server bereit.

Der Serverraum wird hin und wieder durch eine Reinigungskraft gereinigt, dies wird von Fr. Maier überwacht. Bei Gelegenheit, z.B. bei Einbau oder Austausch von Komponenten, werden zentrale Systeme gereinigt
<< 9.mi >> Es erfolgt allerdings keine regelmäßige Reinigung.

Die zentralen Komponenten und Systeme werden durch eine ausreichend dimensionierte USV mit Strom versorgt.
<< 10.mi >> Es ist unklar ob die Server bei längerem Stromausfall automatisch geregelt heruntergefahren werden.

Für wichtige bzw. zentrale Systeme ist ein entsprechender Wartungsvertrag vorhanden welcher die Anforderungen an Verfügbarkeit im Grunde abdeckt. Für den zentralen Sharp Drucker ist ein Wartungsvertrag vorhanden. Der HP Plotter wurde kürzlich gewartet -> kein Wartungsvertrag. Bei Ausfall des Plotters ist der Gang zum Copyshop der entsprechende Workaround.

Die zentralen Server werden nicht speziell gehärtet da aus Kostengründen der Small Business Server eingesetzt wird. Dieser vereint viele Services auf einer Plattform. Das Produkt SBS ist eigentlich für kleine Büros mit ca. 5 Clients dimensioniert.

Alle Systeme, egal ob intern oder extern erreichbar, befinden sich im selben Subnetz. Grund hierfür ist wiederum der Small Business Server.

data security management
data management gmbh
auf der halde 27 0732 791100 - fax dw 25
a-4060 leonding info@datasec.at

Physikalischer Schutz

Der Technikraum in welchem sich die Server und andere Komponenten befinden ist abgesperrt. Fr. Maier besitzt den Schlüssel bzw. gibt es einen Ersatzschlüssel zu welchem die Geschäftsführung Zugriff hat.

Unberechtigte können nicht unbemerkt physikalisch auf die interne IT zugreifen, da bei geöffneter Tür sich immer jemand im Büro befindet.

<< 11.mi >> Der Technikraum ist weder mit einem Brandmelder ausgestattet noch wird die Temperatur automatisch überwacht. Ein CO2 Feuerlöscher steht vor der Tür zum Technikraum. Im Raum sind wasserführende Leitungen vorhanden, welche teilweise direkt über die Server laufen. Im Technikraum wird neben den technischen Komponenten auch Papier gelagert (leicht brennbares Material).

Die Temperatur ist aufgrund der Lage im Keller normalerweise konstant, es ist keine aktive Klimatisierung notwendig. Hochwasser ist laut Fr. Maier kein Problem.

Es gibt eine Alarmanlage für das Büro, welches einen akustischen Alarm auslöst wenn ein Einbruch erkannt wird.

Die wichtigen, zentralen Schlüssel sind jeweils in Kopie sicher verwahrt. Der Zugriff darauf ist nur für die Geschäftsführung möglich.

Externe Dienstleister bzw. der IT Betreuer kann nicht ohne vorherige Anmeldung bei Fr. Maier (-> Schlüssel) auf den Technikraum zugreifen. Der Arbeitsablauf von Dienstleistern im Gebäude wird durch Fr. Maier grundsätzlich verfolgt.

Das Büro kann untertags teilweise von Fremden unbemerkt betreten werden, wenn sich zufällig keiner am Arbeitsplatz aufhält dem dies auffallen würde.

Alte Hardware wird für gewöhnlich im Ganzen entsorgt.
<< 12.mi >> Festplatten oder Wechseldatenträger werden nicht extra ausgebaut oder vorher mechanisch zerstört. Für gewöhnlich befinden sich keine wichtigen Daten auf den lokalen Datenträgern. Der alte Server mit den Projektdaten lagert fürs erste noch im Technikraum.

data security management
data management gmbh
auf der halde 27 0732 791100 - fax dw 25
a-4060 leonding info@datasec.at

Netzwerkverbindungen

Es gibt ein gesichertes WLAN welches laut Fa. Haidmann mittels WAP Verschlüsselung ausreichend geschützt ist.

Zentrale Netzwerkkomponenten wie Switch, Firewall bzw. Internethardware sind relativ neu bzw. können bei Bedarf durch den IT Betreuer rasch ausgetauscht werden.

<< 13.mi >> Die Windows Firewall auf den Clients ist teilweise aktiv, die Standardeinstellung von Windows wurde nicht geändert. Es gibt allerdings keine einheitliche Gruppenrichtlinie welche dies aktiv steuern würde.

Bei den Servern ist die Host Firewall deaktiviert, da der Aufwand für die Feineinstellung aller Services relativ hoch ist. Der Zugriff von extern wird mittels der Juniper Perimeter Firewall geregelt.

data security management
data management gmbh
auf der halde 27
a-4060 leonding
0732 791100 - fax dw 25
info@datasec.at

Internet / Intranet

Das Regelwerk der Firewall ist nach dem „Deny all“ Grundprinzip aufgebaut. Es wird nur erlaubt was unbedingt nötig ist.

Der Zugriff von den Workstations auf das Internet ist mittels Proxy Server geregelt. Dieser ist auch AntiVirus Filter für den Webperimeter -> Trend Micro Suite

Aufgrund des relativ kleinen Regelwerkes der Firewall ist ein regelmäßiges Audit der Firewall-Regeln nicht nötig, Wartung bei Bedarf.

<< 14.mi>> Es wird kein Web-Content Filter eingesetzt welcher unerlaubte Seiten automatisch sperrt.

Spam wird mittels der TrendMicro Suite gefiltert. Dieser arbeitet allerdings nicht optimal. Ein zu restriktives Setting führt zu vermehrten False-Positives, also Nachrichten die legitim sind und dennoch gefiltert werden. Aussage Fr. Maier: „Innerhalb von 3 Tagen kommen dennoch 100 Spam-Mails d11:09hsurch, von denen 75 im Outlook JunkMail Ordner landen.“
<< 15.mi>> Effizientere Lösungen zur Filterung von Spam sind möglich, allerdings läuft der derzeitige Wartungsvertrag für den TrendMicro Filter noch.

Es gibt einige Remote Verbindungen mittels VPN in das interne Netzwerk. Konkret sind das die ARGEn mit Zugriff auf die Transfer Laufwerke. Der Zugriff über die VPN ist, außer in einem Fall, nicht weiter reglementiert – „alles erlaubt“. Die Zugriffs-berechtigungen werden mittels NTFS Berechtigungen festgelegt.
<< 16.mi >> Da die Betreuung der Partner welche sich mittels VPN in das interne Netz einwählen andere als Infoniqa sind, ist nicht klar ob die Systeme der Partner entsprechend geschützt werden. Weiters ist relativ unklar, ob die Systeme der Teleworker auch den aktuellen Sicherheitsanforderungen des Unternehmens genügen (aktueller Virenschutz, aktueller Patchlevel…)

Der Internetanschluss ist mittels xDSL von Tele2 gelöst, der bestehende SLA hierfür ist ausreichend – es gibt keine Backupleitung. Workaround für eine Störung des Internet ist die Verwendung der A1 Datenkarten.
<< 17.mi >> Der Verlust von eingehenden Emails während der Internetstörung ist hierbei die größte Sorge.

Die Telefonanlage wird von einem Bekannten der Geschäftsleitung betreut.
<< 18.mi >> Es ist nicht bekannt inwieweit die Anlage von extern gesteuert werden kann bzw. ob die Zugänge für die Telefonanlage gesichert sind.

data security management
data management gmbh
auf der halde 27 0732 791100 - fax dw 25
a-4060 leonding info@datasec.at

Updates / Sicherheitslücken

Die aktuellen Sicherheitsupdates werden auf den Servern und den Clients mittels WSUS (Update Server für Microsoft Software) entsprechend ausgerollt.

Software welche sich automatisch aktualisieren kann wird auch durch die eingebauten Update-Mechanismen up-to-date gehalten. (Adobe etc.)

<< 19.mi >> Es erfolgt keine Überprüfung auf Schwachstellen und Sicherheitslücken der installierten Software auf Servern bzw. Workstations.

<< 7.ma >> Der IST Zustand des Netzwerkes bzw. möglicher Sicherheits-probleme wird nicht gesondert evaluiert – keine technischen Vulnerability Checks.

Als automatisierte Systeme zur Updateüberwachung bzw. Verteilung wird WSUS eingesetzt.

data security management
data management gmbh
auf der halde 27
a-4060 leonding
0732 791100 - fax dw 25
info@datasec.at

Schutz vor Malware

Auf allen internen Workstations sowie Servern wird TrendMicro als Anti-Malware Software eingesetzt.

Das Management der Software erfolgt über eine Management-Konsole über welche auch eventuelle Probleme mit den verteilten Virenscannern erkannt werden können bzw. diese reportet werden.

Die Aktualisierung der Virenscanner erfolgt über die zentrale Anti-Malware Management Konsole.

Die Mitarbeiter können den Virenscanner nicht manuell deaktivieren, hierfür ist ein Administratorpasswort erforderlich.

data security management
data management gmbh
auf der halde 27
a-4060 leonding
0732 791100 - fax dw 25
info@datasec.at

Conclusio

Die IT Infrastruktur der Firma Max Mustermann GmbH ist bemessen an ihrer Größe und den Anforderungen entsprechend gut aufgestellt und wird auch vom zuständigen IT Betreuer, Fa. Haidmann, kompetent betreut.

Unabhängig dessen sind dennoch einige Schwachpunkte aufgefallen deren weiterführende Betrachtung dringend anzuraten ist.

Für die genauere Analyse dieser Punkte stehen wir Ihnen gerne als Berater zur Seite. Unser Anliegen ist es, in Zusammenarbeit mit dem bestehenden IT Betreuer den „Support Service IT“ für das Unternehmen weiter zu optimieren.

data security management
data management gmbh
auf der halde 27
a-4060 leonding
0732 791100 - fax dw 25
info@datasec.at