

<u>1.) Einleitung</u>	3
<u>2.) Definitionen</u>	3
<u>a) Definition von elektromagnetischer Strahlung</u>	3
Leistung; Frequenz / Wellenlänge, Entstehung an Elektronik	3
<u>b) Definition von Computer (nach VDE)</u>	4
digitale Datenverarbeitungsanlage aus integrierten Schaltungen	4
<u>3.) Grundlagen</u>	4
<u>a) Abschirmung</u>	4
Wie, mit welchen Materialien, wo	4
<u>b) Meßmethoden</u>	5
- elektrische Felder	5
womit nach VDE / TCO, Prinzip	5
- magnetische Felder	6
womit nach VDE / TCO, Prinzip	6
- Wellen	7
womit nach VDE / TCO, Prinzip	7
<u>4.) Warum abschirmen?</u>	8
<u>a) Störung an anderen Geräten</u>	8
Störung bei Rundfunk/TV-Empfang, Störung anderer Computer	8
<u>b) Störung durch andere Geräte</u>	8
Stromleitungen, TV-Geräte, Straßenbahnleitungen, Lautsprecher	8
<u>c) Sicherheit (Datenschutz)</u>	9
TEMPEST (=Lauschen), DOS (=Lahmlegen)	9
<u>d) Einflüsse auf Menschen</u>	9
Elektrosmog, Röntgenstrahlung an Monitoren?	9
<u>5.) Messungen an einem (normalen) PC</u>	10
<u>a) Meßwerte</u>	10
Tabelle	10
<u>b) Meßmethoden</u>	11
Nennung, Vergleich mit VDE / TCO, evtl. Besonderheiten	11
<u>c) Auswertung</u>	12
Quellen, Auswirkungen, Vergleich mit anderen Quellen	12
<u>d) Vergleich mit erhofften / vorgeschriebenen Werten</u>	13
<u>e) Absichtliche Abstrahlung im 10Mhz-Bereich</u>	13

<u>6.) Messungen an einem abgeschirmten PC</u>	15
a) <u>Meßwerte</u>	15
b) <u>Meßmethoden</u>	16
c) <u>Auswertung</u>	16
d) <u>Vergleich mit erhofften/vorherigen Werten</u>	17
<u>7.) Schluß</u>	17
drahtlose Netzwerke	17
<u>A.) Beschreibung des verwendeten Computers</u>	19
a) <u>Komponenten</u>	19
<u>B.) Beschreibung der verwendeten Abschirmmaterialien</u>	19
<u>C.) Literatur / Zitateverzeichnis</u>	20
<u>D.) Beschreibung der verwendeten Software</u>	21

1.) Einleitung

Auf das Thema gekommen bin ich aufgrund meines Interesses für Computersicherheit und einer gewissen Nähe zu den (teils ausgefallenen) Hard- und Softwarebasteleien des ChaosComputerClubs e.V. in Berlin, der sich laut Vereinscharta mit dem kreativen Umgang mit Technik, den gesellschaftlichen Auswirkungen der zunehmenden Technisierung und der Vertretung des Datenschutzes verschrieben hat¹. Dabei stößt jeder, der sich für dieses Gebiet interessiert, über kurz oder lang auf den Begriff TEMPEST (Transient Electromagnetic Pulse Standard)². Dieser beschreibt einen Standard der amerikanischen Regierung für die Messung der elektromagnetischen Emission eines Computers, und wieviel ein (Regierungs)-PC davon abstrahlen darf. 1985 gelang es dem Niederländischen Wissenschaftler Wim van Eck einen TEMPEST-Angriff durchzuführen und er veröffentlichte im "Computers & Security"-Journal den Artikel "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" [Elektromagnetische Strahlung von Bildschirmen: Ein Abhörriisiko?], in dem er beschrieb, daß die von einem Computer ausgehende Strahlung abgefangen, und daß daraus das Monitorbild rekonstruiert werden kann. Dieses Experiment mit heutigen Monitoren und der mir zur Verfügung stehenden Ausrüstung zu wiederholen, schien aussichtslos, aber was ein Computer abstrahlt und was man messen kann, interessierte mich doch. Da der TEMPEST-Standard nicht frei zugänglich ist, beschränke ich mich im folgenden auf die zivilen und frei erhältlichen Standards des VDE (Verband deutscher Elektriker) und des TCO (schwedischer Gewerkschaftsverband).

2.) Definitionen

a) Definition von elektromagnetischer Strahlung

Elektromagnetische Strahlung ist eine Erscheinungsform von freier (also nicht an Materie gebundener) Energie. Typische, sie charakterisierende Größen sind die Ausbreitungsgeschwindigkeit v , die Frequenz f und die Leistung P . Dabei ist für elektromagnetische Strahlung v typischerweise die Lichtgeschwindigkeit und (zumindest für Computer) f zwischen 50 Hertz und einigen Megahertz. Die Leistung P bewegt sich dabei in einem Bereich von einigen Watt. Die elektromagnetische Strahlung entsteht bei Computern hauptsächlich an von Wechselstrom durchflossenen Leitern, insbesondere dann, wenn gilt: Länge des

¹[wch]

²[cth]

Leiterstücks $l = k \cdot \frac{\lambda}{2}$ ($k \in N$) (Resonanzfall, praktischer Nachweis in [rsp]). Da aber vor allem Frequenzen von einigen Kilohertz bis zu ungefähr 200 Mhz auftreten und damit Wellenlängen von einigen Kilometern bis zu einigen Metern, ist der Resonanzfall eigentlich nur an den Kabeln zu den Peripheriegeräten denkbar.

Zusätzlich zur Strahlung finden sich im Nahbereich auch noch elektrische und magnetische Wechselfelder, die aufgrund der höheren Intensität leichter zu messen sind.

b) Definition von Computer (nach VDE)

Der VDE spricht in den relevanten Vorschriften von "informationstechnischen Einrichtungen" und definiert diese über Empfang und Ausgabe von Daten, die Durchführung von Verarbeitungsschritten, die Erzeugung bzw. Verwendung von "binär ... gesteuerten Wellenformen" zum Zwecke z.B. der Textverarbeitung (VDE 0871 Teil 2 2 ITE). Diese Facharbeit beschränkt sich jedoch auf die Standardkomponenten eines handelsüblichen PC (→ *Anhang A*, Beschreibung der verwendeten Hardware).

3.) Grundlagen

a) Abschirmung

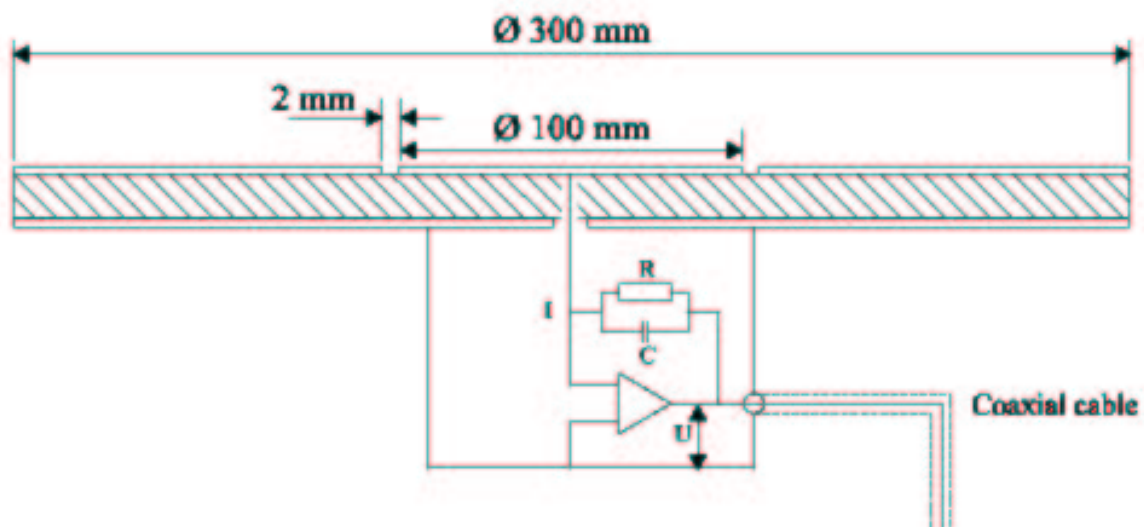
Die Abschirmung erfolgt durch eine geschlossene Hülle aus absorbierenden Materialien um die Störquelle /-senke. Das bedeutet, elektrische Felder werden z.B. durch eine geerdete Hülle aus leitfähigen Materialien um die feldverursachende Ladung abgeschirmt. Des Weiteren würde man die Ecken und Kanten, falls möglich, abrunden, um die Feldstärke an diesen Stellen zu reduzieren bzw. niedrig zu halten, falls die Umhüllung sich doch auflädt. Magnetische Felder sind deutlich schwerer abzuschirmen, da sie im Prinzip nur durch ein gleichstarkes Gegenfeld neutralisiert werden können. Zum Glück treten Magnetfelder an Computern (außer an Bildschirmen) im Vergleich zu anderen elektrischen (Haushalts-)Geräten selten auf. Ebenfalls möglich wäre eine Abschirmung, die dem B-Feld durch ständiges Wechseln der Magnetisierungsrichtung Energie entzieht und in Wärme umwandelt (→ *Anhang B* Beschreibung der verwendeten Abschirmmaterialien). Elektromagnetische Wellen werden, wie E-Felder, durch eine leitende Umhüllung "absorbiert". Diese Hülle muß nicht geerdet sein und darf sogar "Lücken" z.B. für Kabeldurchführungen besitzen (mit $d \ll \lambda$). Für den Ort der Abschirmung gibt es zwei Strategien, entweder möglichst nahe an der Störquelle/ -senke oder eine Abschirmung um die Gesamtanlage. Auf Computer bezogen hieße das, daß man entweder eine einzelne besonders empfindliche Komponente wie

etwa den Prozessor oder eine besonders stark strahlende Komponente wie das Netzteil einzeln abschirmt oder eine Umhüllung um den gesamten Computer verwendet, was aufgrund entfallender Platzprobleme leichter möglich wäre, aber mehr Material verbrauchen würde.

b) Meßmethoden

- elektrische Felder

Die statischen elektrischen Felder kann man allgemein mit einem Influenz-E-Feldmesser messen, homogene Wechselfelder mittels des Verschiebestroms zwischen zwei gegeneinander und gegen Erde isolierten Elektroden. Für die TCO-Messung wird eine Meßsonde folgenden Aufbaus verwendet³.



Zwei kreisförmige ($r=0,15$ m) Kupferfolien sind durch einen einige Millimeter dicken Isolator getrennt. Auf der dem Meßobjekt zugewandten Seite ist eine innere Kreisfläche ($r=5$ cm) durch einen 2mm breiten Spalt vom umgebenden Kreisring getrennt. Zur Messung wird die Rückseite und der äußere Kreisring der Vorderseite an der Abschirmung des Koaxialkabels angeschlossen und damit geerdet, und die kleine Kreisscheibe auf der Vorderseite wird über einen Operationsverstärker mit kapazitiver Rückkopplung als Meßverstärker angeschlossen. Im elektrischen Wechselfeld kommt es bei dieser Anordnung zu Verschiebestromen, die über den Operationsverstärker vorverstärkt werden und dann mit einem Meßverstärker und einem daran angeschlossenen Milliampereometer gemessen werden. Man misst also quasi permanent den Auf-/Entladestrom der Meßfläche gegenüber Erdpotential. Die Stärke des E-Feldes ergibt sich dann zu $E = \frac{U \cdot C}{A \cdot \epsilon_0}$. Dabei ist U die Spannungsdifferenz zwischen Erde

³[sup] S. 13 ff. 2.1 Alternating electric field

und Kreisscheibe, C die Kapazität des Meßverstärkers, A die Fläche der Kreisscheibe und ε_0 ist die elektrische Feldkonstante. Herleiten läßt sich diese Formel über folgende Zusammenhänge⁴: $D = \frac{Q}{A}$, $D = \varepsilon_0 \cdot E$ und $C = \frac{Q}{U}$. Es gilt nämlich, daß $Q = C \cdot U$ und $\frac{Q}{A} = \varepsilon_0 \cdot E$. Daraus ergibt sich $\frac{C \cdot U}{A} = \varepsilon_0 \cdot E$ und damit die oben angegebene Formel. Vor der Messung wird die Sonde im homogenen Feld eines Plattenkondensators bei Frequenzen von 16 - 1000 Hz bzw. 15-120kHz und Feldstärken von 2,5 bis 250 V/m geeicht.

- magnetische Felder

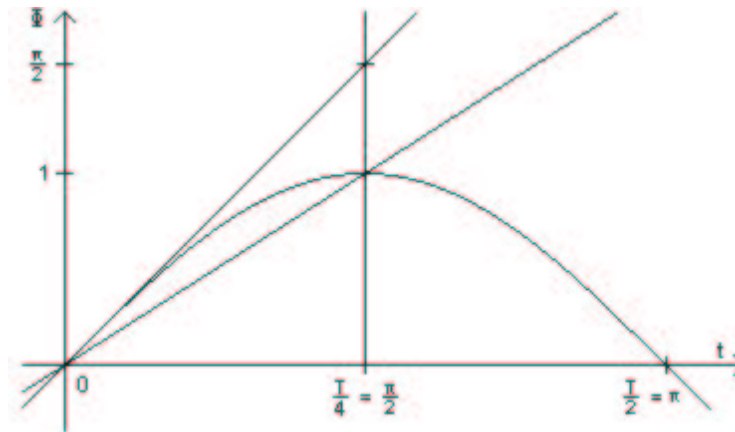
Statische Felder mißt man über Hallsonde, Wechselfelder über Spule oder Rahmenantenne unter Verwendung des Induktionsstromes. In den Meßvorschriften der TCO sind drei zylindrische, rechtwinklig zueinander angeordnete Spulen mit 116mm Durchmesser vorgeschrieben. Die Resonanzfrequenz der Meßsonde muß außerhalb des zu messenden Bandes liegen und durch Widerstände möglichst weit abgedämpft sein. Diese Vorschrift liegt in der physikalischen Beobachtung begründet, daß ein schwingungsfähiges System bei seiner Resonanzfrequenz auch bei einer sehr geringen Zufuhr von Energie zu sehr starken Schwingungen angeregt werden kann. Es könnte also passieren, daß sehr geringe magnetische Felder, die aber die Resonanzfrequenz der Meßsonde treffen, das System soweit aufschaukeln, bis ein falscher, da viel zu hoher Meßwert abgelesen wird. Die Vorschrift, daß die Meßsonde durch Widerstände abgedämpft werden muß, die Resonanzkurve also flachgehalten werden soll, ist aus folgendem Grund sinnvoll. Ein schwingungsfähiges System läßt sich bei gleicher Anregungsamplitude mit Frequenz in der Nähe der Resonanzfrequenz deutlich besser zu Schwingungen anregen, als mit Frequenzen, die sich deutlicher von der Resonanzfrequenz unterscheiden. Wenn die Resonanzfrequenz nun knapp oberhalb der oberen Grenze des Meßfilters und des zu messenden Frequenzbandes läge, würden hohe Frequenzen das System deutlich stärker anregen und damit unverhältnismäßig stark in den Meßwert eingehen. Wenn man aber mit Widerständen die Resonanzkurve stark abdämpft, dann ist die Frequenzabhängigkeit der Empfindlichkeit nicht mehr zu registrieren bzw. nicht mehr störend, da sehr schwach ausgeprägt. Vor der Messung wird die Sonde im sinusmäßig modulierten quasi homogenen Feld eines Helmholtzspulenpaares bei Frequenzen von 16 -1000 Hz bzw. 15-120kHz und Flußdichten von 25 - 2000 nT geeicht. Das Meßprinzip ist hier, daß eine Änderung im Magnetfeld eine Induktionsspannung in der Spule erzeugt. Dabei ist die Höhe der Spannung proportional zur Ableitung der Magnetfeldstärke B nach der Zeit. Da auch die Geschwindigkeit der Änderung bekannt ist (also die Frequenz bzw. Periodenlänge des magn. Feldes und der induzierten Spannung), kann

⁴[pfs] S. 39 f.

man unter der Annahme, daß die Feldstärke einem sinusartigen Verlauf folgt, auch den Spitzenwert des Feldes angeben. Diese vereinfachende Annahme trifft auf die Magnetfelder eines Computers / Monitors sogar relativ gut zu. Die Feldstärke B ergibt sich hier zu:

$$B = \frac{2 \cdot T \cdot U}{\pi^2 \cdot n \cdot d^2}$$

Dabei ist T die Periodendauer des magn. Wechselfeldes, U ist die Induktionsspannung, n die Windungszahl der Spule und d der Durchmesser der Spule. Diese Formel ergibt sich aus den folgenden Ansätzen: Laut Formelsammlung ist $\frac{d}{dt}\Phi = \frac{U}{n}$ und $B = \frac{\Phi}{A}$. Für die Querschnittsfläche der (zylindrischen) Meßspule gilt: $A = \pi \cdot r^2 = \pi \cdot \left(\frac{d}{2}\right)^2 = \frac{\pi}{4} \cdot d^2$. Aus der folgenden Abbildung ergibt sich: $\Phi\left(\frac{T}{4}\right) = \frac{T}{4} \cdot \frac{d}{dt}\Phi \cdot \frac{2}{\pi}$.



$$\Rightarrow B = \frac{4 \cdot \Phi}{\pi \cdot d^2} = \frac{4 \cdot T \cdot \frac{d}{dt}\Phi \cdot 2}{4 \cdot \pi^2 \cdot d^2} = \frac{2 \cdot T \cdot U}{n \cdot \pi^2 \cdot d^2}$$

- Wellen

Die Messung erfolgt hier über (Dipol-)Antennen, die bei $f > 80\text{MHz}$ auf das arithmetische Mittel des zu messenden Frequenzbandes abgestimmt sein müssen, für Frequenzen $f < 80\text{MHz}$ auf 80MHz abgestimmt werden. Es wird entweder die Gesamtleistung gemessen oder das gemessene Signal wird in einzelne Frequenzbänder aufgegliedert (Spektralanalyse). Die Antenne wird dabei so ausgerichtet, daß der höchste Meßwert erreicht wird. Der Boden und die Umgebung des Prüfkörpers muß von reflektierenden Gegenständen frei sein. Die Meßantenne ist über ein geschirmtes Koaxialkabel an das Millivoltmeter (bzw. das gewünschte Meßinstrument) anzuschließen.

4.) Warum abschirmen?

a) Störung an anderen Geräten

Es gibt mehrere Gründe, warum man Computer und andere elektrische Geräte abschirmt und abschirmen muß. Der erste ist: Sämtliche elektrischen/elektronischen Geräte sind Störquellen, die den Betrieb anderer Geräte beeinträchtigen oder gänzlich unmöglich machen können oder sie im schlimmsten Falle sogar zerstören können. Ein typischer solcher Fall sind Tönstörungen an Lautsprechern im Moment der Inbetriebnahme eines Monitors. Um solche Störungen zu minimieren, dürfen elektrische Geräte nur mit CE-Prüfung betrieben werden, was die Einhaltung bestimmter Grenzwerte garantiert. Diese Grenzwerte sollten ursprünglich eine Störung des Rundfunkempfangs verhindern, garantieren heute aber auch z.B. die Verträglichkeit mehrerer Computer. Dabei sind Computer mit Feldstärken $< 10\text{nT}$ im Vergleich zu anderen Haushaltsgeräten mit Feldstärken von bis zu 20 nT (z.B. Fön, Mixer o.ä. motorgetriebene Geräte)⁵ aber (zumindest theoretisch) relativ unproblematisch.

b) Störung durch andere Geräte

Ein weiterer Grund für eine Abschirmung ist, daß elektrische Geräte sich nicht stören lassen sollen z.B. durch nah vorbeilaufende Stromkabel (eines anderen Gerätes, einer Straßenbahn...) oder die Magnetfelder von Lautsprechern. Ein typisches Beispiel dieser Art sind Bildverzerrungen und Farbveränderungen auf einem Monitor, der in der unmittelbaren Nähe eines Lautsprechers steht. Dieses Problem tritt bei moderneren Monitoren (dank besserer Abschirmung) seltener auf, ist aber z.B. bei schlechten Lautsprechern oder in unmittelbarer Nähe zu Bahnstrecken immer noch zu beobachten. Computer sind gerade in diesem Bereich im Vergleich zu anderen Geräten empfindlich, da ein Großteil der Informationen in magnetischer Form, etwa auf Disketten oder Festplatten, abgelegt ist und eine Verfälschung, Beeinflussung oder Löschung dieser Daten den Betrieb trotz der vorhandenen fehlerkorrigierenden Codes rasch unmöglich macht. Auch der in elektrischer Form abgelegte Teil der Daten ist sehr empfindlich gegenüber Verfälschungen, was aber heute z.B. durch integrierte Abschirmungen und Fehlerkorrektur direkt in den RAM-Modulen wenig Probleme bereitet. Gut zu erkennen ist diese Abschirmung vor allem bei Speichermodulen nach dem Rambusstandard, da sie hier oft als metallische Abschirmschicht um das Modul ausgeführt ist⁶.

⁵[urp] 12/2001 Nr. 65 S. 49

⁶z.B. [tir]

c) Sicherheit (Datenschutz)

Ein weiterer, aber oft übersehener Beweggrund ist die Sicherheit des Computers und der darauf gespeicherten Daten. Hier muß zwischen einem aktiven Angriff und einem passiven Mithören unterschieden werden. Bei einem aktiven Angriff werden Signale in Form von elektromagnetischen Wellen oder von drahtgebundenen Störungen abgegeben, um Daten oder Ergebnisse zu verfälschen oder den Computer zu (zer)stören. Die Möglichkeit wurde erstmals im Rahmen der Untersuchung des EMP (elektromagnetischen Pulses) einer Atombombe erwähnt. Durch die steigende Komplexität und damit Empfindlichkeit der elektronischen Baugruppen und der gestiegenen Leitungsfähigkeit der Leistungselektronik geht man heute davon aus, daß mittels eines portablen Signalgenerators ungeschützte Computer in einer Entfernung von ca. 30m betriebsunfähig gemacht werden können. Im Gegensatz dazu wird bei einem passiven Angriff nicht aktiv manipuliert, sondern es werden nur die von einem Computer ausgehenden Signale analysiert, um Bildschirm-, Tastatur- oder Mausdaten und damit Passwörter, vertrauliche Daten o.ä. zu erhalten. Gerade nicht kabelgebundene Übertragungsverfahren wie z.B. bei Funktastaturen sind für solche “Angriffe” anfällig. Auch die steigende Verwendung von Funknetzwerkkarten, nach dem IEEE 802.11b Standard⁷, und die damit verbundene (hier sogar beabsichtigte) Abstrahlung von Daten eröffnen quasi täglich neue Problemgebiete, die bisher noch kaum wahrgenommen werden. Interessant sind in dieser Richtung vor allem die Ergebnisse, die einige Mitglieder des ChaosComputerClubs beim “war driving” hatten. Als “war driving” bezeichnet man den Vorgang, mit einem Notebook mit Funknetzwerkkarte und geeigneter Software⁸, die sämtlichen Netzwerkverkehr auf Festplatte in eine Datei schreibt, durch eine Gegend zu gehen, in der man offene Funknetze vermutet. Bei diesem “war driving” wurden inzwischen gerade in den Großstädten viele unzureichend abgesicherte Netze etwa von Banken und Kliniken gefunden, durch die teilweise sehr sensible Informationen transportiert werden.

d) Einflüsse auf Menschen

Die Störwirkung von Feldern und Wellen ist nicht auf andere elektrische Gerät beschränkt, sondern auch organisches Gewebe und damit der Mensch sind für gewisse Störungen empfindlich. Die genauen Auswirkungen und Grenzwerte werden kontrovers diskutiert, gerade deshalb aber sollte man bestrebt sein, die mögliche Belastung so gering wie möglich

⁷[sip]

⁸z.B. [moh], [ash]

zu halten. Als gesichert können jedoch z.B. Ermüdungserscheinungen durch starke elektrische Wechselfelder und die Gefährdung durch Röntgenstrahlen (an Monitoren) gelten. Hier können durch geeignete Abschirmungen und andere Maßnahmen (z.B. Begrenzung der Beschleunigungsspannung) die Grenzwerte relativ einfach eingehalten werden. Die TCO99-Norm schreibt hier etwa die Unterschreitung von 5000 nGy/h vor⁹.

5.) Messungen an einem (normalen) PC

a) Meßwerte

E/M	C/M	v/l/h	f	d	Meßwert	TCO
E	C	v	5 Hz - 2 kHz	0,30 m	0,7 V/m	10 V/m
E	C	v	5 Hz - 2 kHz	0,50 m	0,5 V/m	
E	C	v	2 - 400 kHz	0,30 m	0 V/m	1.0 V/m
E	C	l	2 - 400 kHz	0,50 m	0 V/m	1.0 V/m
E	C	h	2 - 400 kHz	0,50 m	0 V/m	1.0 V/m
M	C	v	5 Hz - 2 kHz	0,30 m	24 nT	200 nT
M	C	l	5 Hz - 2 kHz	0,50 m	11 nT	200 nT
M	C	h	5 Hz - 2 kHz	0,50 m	18 nT	200 nT
M	C	v	30 Hz - 30 kHz	0,50 m	13 nT	25 nT
M	C	l	30 Hz - 30 kHz	0,50 m	9 nT	25 nT
M	C	h	30 Hz - 30 kHz	0,50 m	14 nT	25 nT
E	M	v	5 Hz - 2 kHz	0,30 m	6,0 V/m	10 V/m
E	M	l	5 Hz - 2 kHz	0,50 m	1,1 V/m	10 V/m
E	M	h	5 Hz - 2 kHz	0,50 m	1,2 V/m	10 V/m
E	M	v	2 - 400 kHz	0,50 m	0,0 V/m	1.0 V/m
E	M	l	2 - 400 kHz	0,50 m	0,1 V/m	1.0 V/m
E	M	h	2 - 400 kHz	0,50 m	0,2 V/m	1.0 V/m
M	M	v	5 Hz - 2 kHz	0,30 m	96 nT	200 nT
M	M	l	5 Hz - 2 kHz	0,50 m	87 nT	200 nT
M	M	h	5 Hz - 2 kHz	0,50 m	57 nT	200 nT
M	M	v	30 Hz - 30 kHz	0,50 m	34 nT	25 nT
M	M	l	30 Hz - 30 kHz	0,50 m	92 nT	25 nT
M	M	h	30 Hz - 30 kHz	0,50 m	52 nT	25 nT

Legende:

E/M in der ersten Spalte bezeichnet, ob elektrische oder magnetische Felder gemessen werden.

C/M in der zweiten Spalte bezeichnet, ob am Computer oder am Monitor gemessen wird.

⁹[crp] S.10 4.1 X-Ray Radiation

v/l/h in der dritte Spalte gibt an, ob vorne, an der linken Seite oder hinten am Gerät gemessen wird.

Die vierte Spalte gibt den Frequenzbereich bei der Messung an.

In der fünften Spalte ist der Abstand von Gehäuseoberfläche zum Meßgerät angegeben.

Die vorletzte Spalte enthält den abgelesenen Meßwert.

In der letzten Spalte, steht der Wert, der laut TCO99¹⁰ maximal erlaubt ist.

b) Meßmethoden

Die E-Felder wurden mit einer Sonde



entsprechend der TCO gemessen. Dabei waren die Abschirmung bzw. das Gehäuse und die Sonde über denselben Erdungspunkt geerdet, um systematische Meßfehler wie elektrostatische Aufladungen oder durch Erdschleifen zu verhindern. Für die Messung der Magnetfelder wurde eine Meßsonde

¹⁰[crp] bzw. [sup]



eingesetzt, die drei orthogonal zueinander angeordnete Meßspulen enthält. Die Sonde ist aber zu klein ($d_{Spule} < 7cm$), um strikt TCO-konform zu sein. Zudem ist der obere Meßbereich auf 30 Hz - 30 kHz anstatt der vorgeschriebenen 2 - 400 kHz eingeengt.

c) Auswertung

Auffallend ist besonders die Stärke der elektrischen Felder vorne am Monitor, die zwar noch im Rahmen der TCO99-Norm ist, aber mit 6 V/m sich doch deutlich von den an anderer Stelle gemessenen 1-2 V/m abheben. Der Grund dafür ist das sehr geringe Vorkommen von Metallteilen an der Frontseite des Monitors, die abschirmend wirken könnten. Die einzigen metallischen Anteile sind hier in der Lochmaske enthalten, die nur einige Zehntelmillimeter dick ist, während das restliche Gehäuse eine Dicke von einigen Millimetern aufweist. Auffallend ist auch die geringe Feldstärke der elektrischen Felder rund um den Computer. Hier sind Werte von unter 1 V/m zu registrieren, während bei dem Computer, der für die erste Testmessung verwendet wurde, Werte von bis zu 20 V/m gemessen wurde. Diese deutlichen Unterschiede liegen in der Verarbeitungsqualität und den verwendeten Materialien der beiden Gehäuse begründet. Während das bessere Gehäuse vollständig aus Metallteilen mit gut leitendem Kontakt zwischen den Einzelteilen besteht, ist das andere Gehäuse zum Teil aus Plastikelementen aufgebaut, die an der Innenseite mit einer elektrisch leitenden Schicht besprüht sind und teilweise keinen leitenden Kontakt zueinander besitzen. Zudem enthält das bessere Gehäuse fast keine Öffnungen; das andere Gehäuse hingegen besitzt an der Frontseite eine große Öffnung für Laufwerkseinschübe, die nur mit Kunststoff-Sichtblenden abgedeckt ist.

d) Vergleich mit erhofften / vorgeschriebenen Werten

Beim Vergleich mit den Werten, die in der TCO99-Norm genannt werden, ist einzig und allein der Wert für die magnetischen Wechselfelder am Monitor im Frequenzband von 2 - 400 kHz zu hoch. Erlaubt wären 25 nT¹¹, es werden jedoch bis zu 92 nT erreicht. Der Monitor ist aber aus dem Jahr 1997 und hält laut Hersteller die Werte der TCO92-Norm ein, die im Laufe der Zeit bis zur TCO99-Norm immer weiter verschärft wurden.

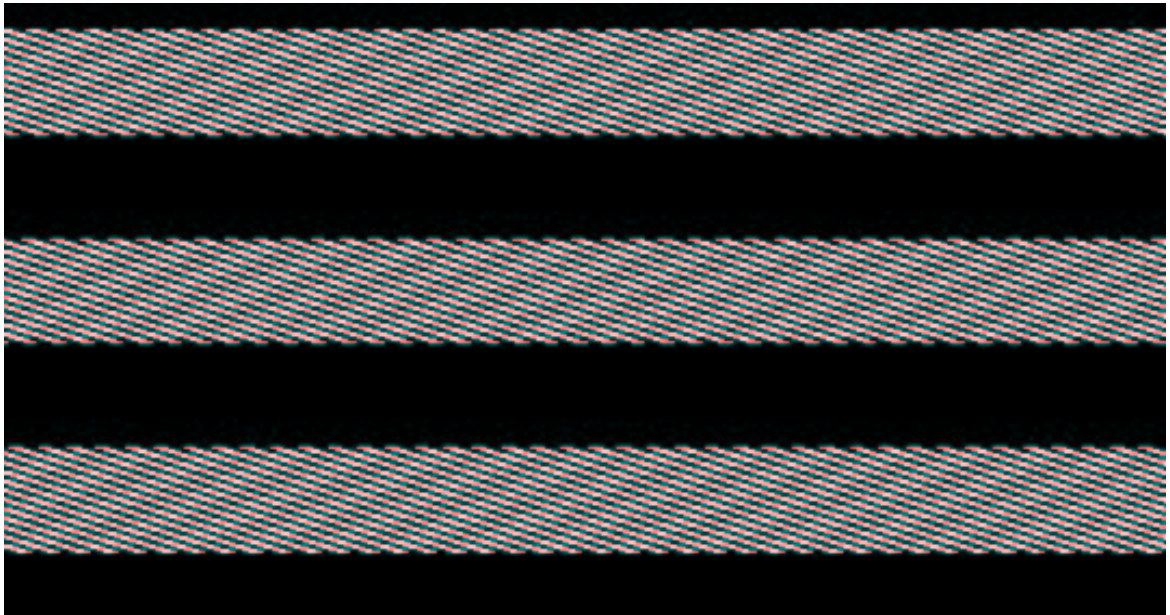
Bei den Messungen am Computer hat sich gezeigt, dass alle Meßwerte im Rahmen der TCO99-Norm liegen. Andererseits wurde ein großer Teil der vorgeschriebenen Messungen (z.B. Lautstärke und Energiesparmodi¹²) nicht durchgeführt, so daß man nicht automatisch davon ausgehen kann, daß der Computer konform zur TCO99-Norm ist.

e) Absichtliche Abstrahlung im 10MHz-Bereich

Mittels geeigneter Computerprogramme (\rightarrow *Anhang D*, Beschreibung der verwendeten Software) ist es leicht möglich, den Elektronenstrahl in der Bildröhre so zu manipulieren, daß ein nach dem Verfahren der Amplitudenmodulation modulierte Tonsignal abgestrahlt wird. Dieses Signal ist bis in einige Meter Entfernung zu empfangen. Dabei kommt das Trägersignal durch schnelle hell/dunkel Pixelwechsel (etwa 5 weiß, 5 schwarz,...), das Audiosignal wird darauf aufmoduliert, indem über mehrere Zeilen hinweg der Kontrast moduliert wird (einige Zeilen schwarz/weiß Wechsel, dann einige Zeilen konstant schwarz). Der Monitor erzeugt dieses Bild, in dem er die Stärke des Elektronenstrahls verändert und damit die Stärke der Abstrahlung, die vom Elektronenstrahl ausgeht.

¹¹[crp] S.13 4.4 Alternating Magnetic Fields

¹²[sup] S.7 f. 2.3 Energie saving & 4.1 Acoustic Noise



Angeblich existieren Programme, die dies auch für die Abstrahlung der CPU realisieren, um auf den Strombedarf in einzelnen Teilen des Prozessors zurückzuschließen. Dies war aber nicht zu verifizieren und es ist auch fraglich, ob der Prozessor eine ähnlich starke Abstrahlung wie der Monitor erreichen kann.

6.) Messungen an einem abgeschirmten PC

a) Meßwerte

E/M	C/M	v/l/h	f	d	Meßwert	TCO
E	C	v	5 Hz - 2 kHz	0,30 m	0,5 V/m	10 V/m
E	C	v	5 Hz - 2 kHz	0,50 m	0,6 V/m	
E	C	v	2 - 400 kHz	0,30 m	0 V/m	1.0 V/m
E	C	l	2 - 400 kHz	0,50 m	0 V/m	1.0 V/m
E	C	h	2 - 400 kHz	0,50 m	0 V/m	1.0 V/m
M	C	v	5 Hz - 2 kHz	0,30 m	23 nT	200 nT
M	C	l	5 Hz - 2 kHz	0,50 m	14 nT	200 nT
M	C	h	5 Hz - 2 kHz	0,50 m	26 nT	200 nT
M	C	v	30 Hz - 30 kHz	0,50 m	13 nT	25 nT
M	C	l	30 Hz - 30 kHz	0,50 m	10 nT	25 nT
M	C	h	30 Hz - 30 kHz	0,50 m	17 nT	25 nT
E	M	v	5 Hz - 2 kHz	0,30 m	1,2 V/m ¹	10 V/m
E	M	l	5 Hz - 2 kHz	0,50 m	0,6 V/m ²	10 V/m
E	M	h	5 Hz - 2 kHz	0,50 m	0,5 V/m ³	10 V/m
E	M	v	2 - 400 kHz	0,50 m	0,1 V/m	1.0 V/m
E	M	l	2 - 400 kHz	0,50 m	0,0 V/m	1.0 V/m
E	M	h	2 - 400 kHz	0,50 m	0,0 V/m	1.0 V/m
M	M	v	5 Hz - 2 kHz	0,30 m	114 nT	200 nT
M	M	l	5 Hz - 2 kHz	0,50 m	95 nT	200 nT
M	M	h	5 Hz - 2 kHz	0,50 m	50 nT	200 nT
M	M	v	30 Hz - 30 kHz	0,30 m	41 nT	25 nT
M	M	l	30 Hz - 30 kHz	0,50 m	93 nT	25 nT
M	M	h	30 Hz - 30 kHz	0,50 m	53 nT	25 nT

E/M	C/M	v/l/h	f	d	Meßwert	TCO
E	C	v	5 Hz - 2 kHz	0,50 m	0,5 V/m ⁴	10 V/m
E	C	v	2 - 400 kHz	0,50 m	0 V/m	1.0 V/m

1: Bei ungeerdeter Abschirmung: 2,4 V/m

2: Bei ungeerdeter Abschirmung: 1,4 V/m

3: Bei ungeerdeter Abschirmung: 1,2 V/m

4: Bei ungeerdeter Abschirmung: 0,6 V/m

Legende:

E/M in der ersten Spalte bezeichnet, ob elektrische oder magnetische Felder gemessen werden.

C/M in der zweiten Spalte bezeichnet, ob am Computer oder am Monitor gemessen wird. v/l/h in der dritte Spalte gibt an, ob vorne, an der linken Seite oder hinten am Gerät gemessen wird.

Die vierte Spalte gibt den Frequenzbereich bei der Messung an.

In der fünften Spalte ist der Abstand von Gehäuseoberfläche zum Meßgerät angegeben.

Die vorletzte Spalte enthält den abgelesenen Meßwert.

In der letzten Spalte, steht der Wert, der laut TCO99¹³ maximal erlaubt ist.

b) Meßmethoden

Die Meßmethoden sind im Wesentlichen identisch zu denen, die bei der Messung im unabgeschirmten Zustand verwendet werden. Einziger Unterschied ist, daß der Abstand zwischen Meßsonde und Abschirmung und nicht bis zur Gehäuseoberfläche gemessen wurde. Zudem war die Abschirmung geerdet, was beim Monitor im Normalzustand evtl. nicht der Fall ist (das Metallgehäuse befindet sich innerhalb eines Plastikgehäuses, daher ist eine mögliche Erdung nicht zu erkennen).

c) Auswertung

Die Unterschiede bei den Messungen der magnetischen Wechselfelder sind wohl auf Messungenauigkeiten und kleine unvermeidbare Veränderungen am Meßplatz zurückzuführen. Im Bereich der elektrischen Wechselfelder am Computer ist die Auswirkung der zusätzlichen Abschirmung sehr gering, was vermutlich im guten Gehäuse des verwendeten Computers begründet liegt. Dieses Gehäuse ist, anders als bei dem für die Vormessungen verwendeten Computer, komplett aus Metall und besitzt außer an den Laufwerkseinschüben (CD-ROM, u.ä.) keine nennenswerten Öffnungen. Dieses Gehäuse schirmt also elektrische Wechselfelder sehr gut ab, so daß die zusätzliche Abschirmung fast nichts mehr abschirmen kann. Dies ist auch daran erkenntlich, daß bereits im unabgeschirmten Zustand die Werte unter der Detektionsgrenze des Meßgerätes lagen. (Eingetragen als 0,0 V/m, da die exakte Höhe der Meßschwelle nicht bekannt ist.) Beim Monitor konnte jedoch an einigen Stellen eine Verbesserung erreicht werden. Vor allem im Frontbereich, der im Normalbetrieb absolut unabgeschirmt ist, war eine deutlich Reduktion (6,0 V/m \rightarrow 1,2 V/m) zu beobachten. Auch hier konnte keinerlei Abschirmwirkung auf magnetische Felder nachgewiesen werden. Der Grund dafür ist die niedrige Permeabilität. Das verwendete hexagonale Drahtgitter ist wie auch Kupfer ein weichmagnetischer Stoff, bei dem die Abschirmung, also der Anteil an

¹³[crp] bzw. [sup]

Feldenergie, der in Wärme ungewandelt wird, gering ist. Für die Feldstärke außerhalb der Abschirmung gilt: $B_a = \frac{B_i}{1+N\cdot\chi}$ ¹⁴. Dabei ist B_i die Feldstärke im Inneren der Abschirmung, N ist ein dimensionsloser Zahlfaktor namens Entmagnetisierungsfaktor, der sich aus der geometrischen Form der Abschirmung ergibt, und χ ist die Suszeptibilität, die sich zu $\mu_r - 1$ ergibt. Dieses μ_r ist wie auch bei Kupfer unter eins, bei Eisen, einem ferromagnetischen Stoff mit guter Abschirmwirkung, aber bei $\gg 1000$. Eisen läßt sich also sehr gut und sehr stark magnetisieren, jeder Magnetisierungsvorgang entzieht dem magnetischen Wechselfeld aber Energie, die das Eisen in Form von Wärme abstrahlt, und schwächt es dadurch, so daß außerhalb der Abschirmung eine deutlich niedrigere Feldstärke herrscht als innerhalb.

d) Vergleich mit erhofften Werten

Am Computer konnte leider keine deutliche Verbesserung erzielt werden, was auch am guten Gehäuse des Computers liegt (\rightarrow 5.) c)).

Beim Monitor hingegen konnte für die elektrischen Felder eine deutliche Verbesserung besonders im Frontbereich erzielt werden. Dort sank der Wert von 6 V/m auf 1,2 V/m, also ein Fünftel der Feldstärke. An den andern Meßpunkten sank die Feldstärke auch, aber mit 1,1 V/m auf 0,6 V/m und 1,2 V/m auf 0,5 V/m bei weitem nicht so deutlich ("nur" eine Reduktion auf 55 % bzw. 42 % des Ausgangswertes). Diese Werte sind aber mit Vorsicht zu genießen, da sie in der Größenordnung der Meßgenauigkeit liegen.

7.)Schluß

Drahtlose Netzwerke nach dem IEEE-Standard 802.11b¹⁵, besser bekannt als Wireless LocalAreaNetwork oder WLAN, sind zur Zeit auf dem Vormarsch, und werden das weiter sein, obwohl ihre Verwendung einige Fragen aufwirft. Während es bei einem konventionellen drahtgebundenem Netzwerk relativ leicht möglich ist zu kontrollieren, welche Personen und Computer Zugang haben, ist das bei Funknetzen deutlich schwerer. Eines der Ziele von Funknetzen ist (im so genannten "ADHOC-Modus") die Vernetzung mehrerer Computer ohne jeglichen Verwaltungsaufwand. Dies bedeutet jedoch, daß jeder, egal ob befugt oder unbefugt, sich in ein solches Netz einklinken kann, ohne daß seine Präsenz festzustellen wäre, wenn er bzw. sein Computer sich nicht freiwillig meldet. D.h. man kann nie sicher gehen, ob nicht zusätzliche "Kommunikationspartner" vorhanden sind, die man eigentlich nicht "eingeladen" hat. Diese grundsätzliche Schwäche von Funknetzen war auch zum Zeit-

¹⁴[fap] Band II, magnetische Schirmwirkung

¹⁵[sip]

punkt der Normierung bekannt, weswegen Abhilfe in Form von Wire Equivilant Privacy-Verschlüsselung (meist WEP genannt) geschaffen werden sollte. In der Implementierung dieses Verfahrens wurde jedoch mittlerweile ein Fehler gefunden¹⁶, der es erlaubt, binnen kürzester Zeit den Klartext-Datenstrom mitzulesen¹⁷. Viel interessanter als die technischen Einzelheiten sind die Auswirkungen dieser Schwachstellen. Denn diese Funknetze werden nicht nur von Heimanwendern verwendet, sondern auch und gerade von Firmen, Behörden und Kliniken¹⁸, die in Unkenntnis der Problematik wichtige Daten über diese Netze transferieren. Bisher ist dieses Problem außerhalb der Gemeinschaft von Leuten, die sich mit Computersicherheit auseinandersetzen, wenig bekannt, was auch daran liegt, daß bisher noch kein Fall bekannt ist, wo eine solche Lücke ausgenutzt wurde, um einer Firma z.B. finanziellen Schaden zuzufügen. Doch sollte ein solcher Fall bekannt werden, dann ist mit mehreren Folgen zu rechnen. Die wahrscheinlich schnellste Folge wäre, daß der Aktienkurs der betreffenden Firma zusammen mit dem Vertrauen in diese Firma zusammenbrechen würde. Allein dies könnte im schlimmsten Fall ausreichen, um die Firma in den Bankrott zu treiben. Zusätzlich wäre die betroffene Firma von Schadensersatzklagen bedroht, falls z.B. vertrauliche Daten über Versicherungsnehmer oder Patienten auf diesem Weg bekannt würden. Des Weiteren würden sich die Hersteller der Funknetzwerk-ausrüstung einer Flut von Klagen und der Forderung nach Nachbesserung gegenüber gestellt sehen. Alles in allem würde ein solcher Fall einen immensen wirtschaftlichen Schaden, auch durch den Vertrauensverlust bei den Kunden, verursachen. Zum Glück haben einige Firmen und Hersteller von Funknetzwerk-karten begonnen, für Abhilfe zu sorgen. Doch bis diese Maßnahmen, wie z.B. Verschlüsselung der übertragenen Daten auf höheren Protokollebenen oder mit anderen Algorithmen greifen, könnte es bereits zu spät sein.

¹⁶[clh]

¹⁷[ibh]

¹⁸[wlh]

A.) Beschreibung des verwendeten Computers

Der verwendete Computer enthielt die folgenden Komponenten:

- Monitor: Belinea 107010, laut Hersteller Tco 92-konform und CE-geprüft
- Motherboard: P5VX-Be von Asus
- Prozessor: Intel Pentium mit 166 MHz Taktfrequenz
- Laufwerke: 2x Festplatte von Seagate, Diskettenlaufwerke und CD-ROM-Laufwerk
- Netzteil: PACOMP 115 W
- Gehäuse: PACOMP (mit CE-Prüfzeichen)

B.) Beschreibung der verwendeten Abschirmmaterialien

Kupfer:

Kupfer habe ich deshalb als ein Abschirmungsmaterial gewählt, da es gut zu verarbeiten ist. Es läßt sich relativ leicht biegen und abkanten. Zudem ist es leicht erhältlich (etwa von einer Spenglerei) und billig. Es leitet Strom sehr gut (spezifischer Widerstand $\rho = 0,017 \cdot 10^{-6} \Omega m$) und eignet sich daher gut zur Abschirmung von elektrischen Feldern und elektromagnetischen Wellen. Unglücklicherweise besitzt es nicht die hohe Permeabilität eines ferromagnetischen Stoffes, so daß es sich nicht zur Abschirmung von Magnetfeldern eignet.

“Kaninchengitter”:

Ein handelsübliches Drahtgeflecht ist noch einfacher erhältlich und zu verarbeiten als Kupfer. Die Leitfähigkeit ist etwas geringer, die Permeabilität ist leider wie auch bei Kupfer sehr niedrig. Die relativ großen Maschen ($d \approx 3 \text{ cm}$) haben auf die Abschirmwirkung für E-Felder im Vergleich zu Kupfer fast keine Wirkung. Auch die Wirkung auf Wellen ist nicht stark beeinträchtigt, da die Wellenlängen im Meter bis Kilometer-Bereich liegen.



C.)Literatur / Zitatenverzeichnis

Kürzel	Quelle
ash	airsnort.sourceforge.net
clh	www.cryptolabs.org/wep/WeisWEPcccDatenschleuder.html
crp	www.tco-info.com/i/dok99/99crt.pdf
cth	www.attrition.org/~modify/texts/vaneck/c_tempest.html
fap	Fachlexikon ABC Physik vom Harri Deutsch Verlag Frankfurt am Main von 1974
ibh	www.informatik.hu-berlin.de/~thalheim/18c3/index.html
moh	www.monkey.org/~dugsong/dsniff
pfs	Physikalische Formeln und Tabellen, Lindauer Verlag München, von ⁵ 1989
rsp	jya.com/rs232.pdf
sip	standards.ieee.org/reading/ieee/std/lanman/802.11-1999.pdf
sup	www.tco-info.com/i/dok99/99su.pdf
tir	www6.tomshardware.com/mainboard/00q1/000308/images/rambus.jpg
urp	Unterricht Physik
wch	www.ccc.de
wlh	www.ccc.de/wlan

Weiterhin verwendete Literatur und Quellen:

www.pci-card.com/ce.htm
www.apogeonline.com/libri/00483/allegati/doc/tempest/EMP.HTM
jya.com/emr.pdf
www.sozialnetz-hessen.de/ergo-online/Arbeitsplatz/Hardware/G_Pruef-s.htm
www.infowar.com/class_3/harden.html-ssi
www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf
cryptome.org/nsa-94-106.htm
cryptome.org/nstissi-7000.htm
www.fc.net/phrack/files/p44/p44-10.html
www.proton-usa.com/service/pc-tech.htm
www.tco.se/pdfarkiv/TCOenglish.pdf
www.eskimo.com/~joelm/tempestintro.html

Vielen Dank an:

- Martin Schauer, für die Möglichkeit mit seinen Geräten und seiner Mithilfe die nötigen Messungen durchzuführen
- Herrn Berger, für die Betreuung der Facharbeit
- Meine Mutter, für die Korrektur der zahllosen Rechtschreibfehler
- Tilman Frosch, für die Idee über dieses Thema zu schreiben

D.)Beschreibung der verwendeten Software

- Textgestaltung: KLyx und LaTeX
- Bildbearbeitung: gimp
- Messung: tempest for eliza"von www.erikyyy.de

Eigenständigkeitserklärung:

Ich erkläre, daß ich die Arbeit ohne fremde Hilfe angefertigt und nur die im Literaturverzeichnis angeführten Quellen und Hilfsmittel benützt habe.

Eisingen, den