7. Betrachtung von aufbereiteten Testergebnissen am Beispiel aktueller VTC-Tests

In diesem Kapitel sollen einige der in Kapitel 6 vorgestellten Erweiterungen, insbesondere die grafische Darstellung der Ergebnisse und die Betrachtung von Ergebnissen mehrerer Tests (sogenannte Zeitreihen), an den Testergebnissen aktueller VTC-Tests aufgezeigt werden. Abschnitt 7.1 visualisiert die Testergebnisse des Tests 2002-03 (Heureka II). Abschnitt 7.2 visualisiert die Testergebnisse des Tests 2001-10 und vergleicht die Erkennungsraten der Produkte unter den verschiedenen Windows32-Betriebssystemen[93]. Abschnitt 7.3 zeigt Zeitreihen von bisher nicht langfristig in der Entwicklung betrachteten Malware-Datenbanken und visualisiert die Entwicklung der durchschnittlichen Erkennungsrate von bösartiger Software verschiedener Plattformen unter DOS.

Sämtliche Tabellen und Grafiken dieses Kapitels sind durch die Datenbank VTED erstellt worden. Dieses Kapitel zeigt somit auch den praktischen Nutzen der im Rahmen dieser Arbeit entwickelten Verbesserungen und Erweiterungen für das VTC-Verfahren. Die genauen Produktbezeichnungen zu den in den jeweiligen VTC-Tests verwendeten Abkürzungen finden sich in Anhang A.

7.1 Grafiken zum Test 2002-03 (Heureka II)

Der Test 2002-03 ist der zweite sogenannte Heureka-Test (nach Heureka I 2001-07), bei dem die Erkennung von Malware mit veralteten Signaturen getestet wird. Dazu werden die Produkte mit dem Aktualisierungsstand des jeweils vorherigen VTC-Tests benutzt. Mit diesen nicht aktualisierten Produkten werden dann (nur unter Windows NT) aktuelle Datenbanken überprüft. Die Erkennung wird nur auf Skript- und Makro-Malware getestet und zwar jeweils mit Datenbankstand von drei und sechs Monaten nach Erhalt der Produkte (*submission deadline*). Dementsprechend besitzen die Datenbanken beim Test Heureka II den Zusatz Juli und Oktober, je nachdem, ob es sich um den Datenbankstand von Juli oder Oktober handelt.

Die Produktsignaturen sind von Ende Juni 2001 (*submission deadline*: 25. Juni 2001). Da die Produkte im Vergleich zu den Datenbanken nicht auf dem aktuellen Stand sind, ist eine Abnahme der Erkennungsrate von Juli bis Oktober nicht verwunderlich. Die Erkennungsraten auf folgenden Datenbanken - aller im Test Heureka II verwendeten - werden in Ergebnisgrafiken jeweils für den Datenbankstand Juli und Oktober gegenübergestellt:

- Makro-Itw

[93]Getestete Windows32-Betriebssysteme sind Windows98, WindowsNT und Windows2000; das heißt Windows-Betriebssysteme, die 32-bit-Adressierung unterstützen

- Makro-Zoo
- Makro-Malware
- Skript-Itw
- Skript-Zoo
- Skript-Malware

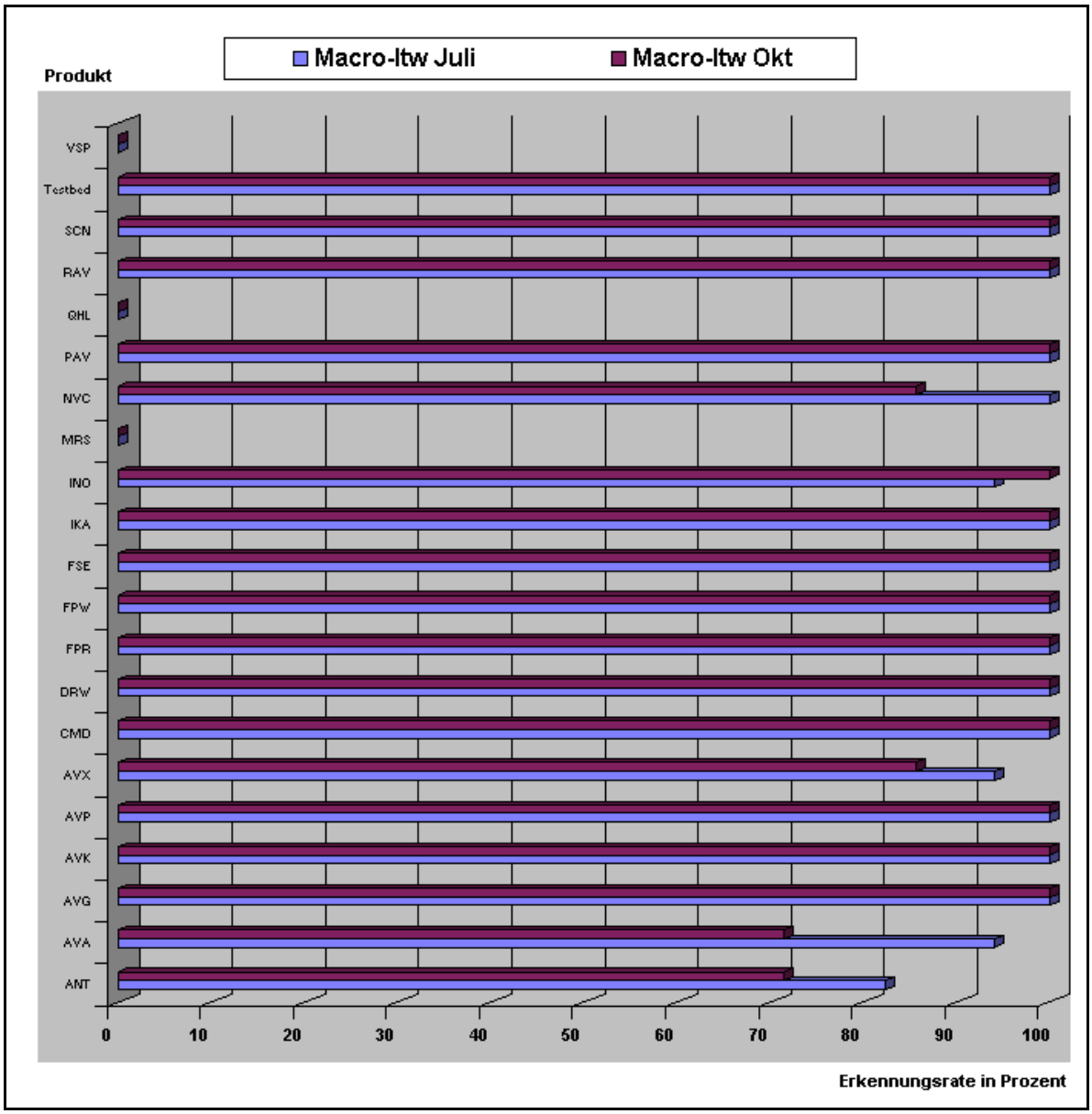

Abbildung 7.A: Entwicklung der Macro-Itw Erkennung im Test 2002-03

Abbildung 7.A vergleicht die Makro-Itw Erkennungsrate zwischen Juli und Oktober. Erstaunlich viele Produkte erkennen selbst im Oktober noch alle (100%) der als Itw eingestuften Viren. Dies liegt darin begründet, daß viele Itw-Viren in den Monaten zuvor

schon als Zoo-Viren bekannt sind und die entsprechenden Produkte eine gute Zoo-Erkennung zum Zeitpunkt der letzten Signaturaktualisierung besaßen.

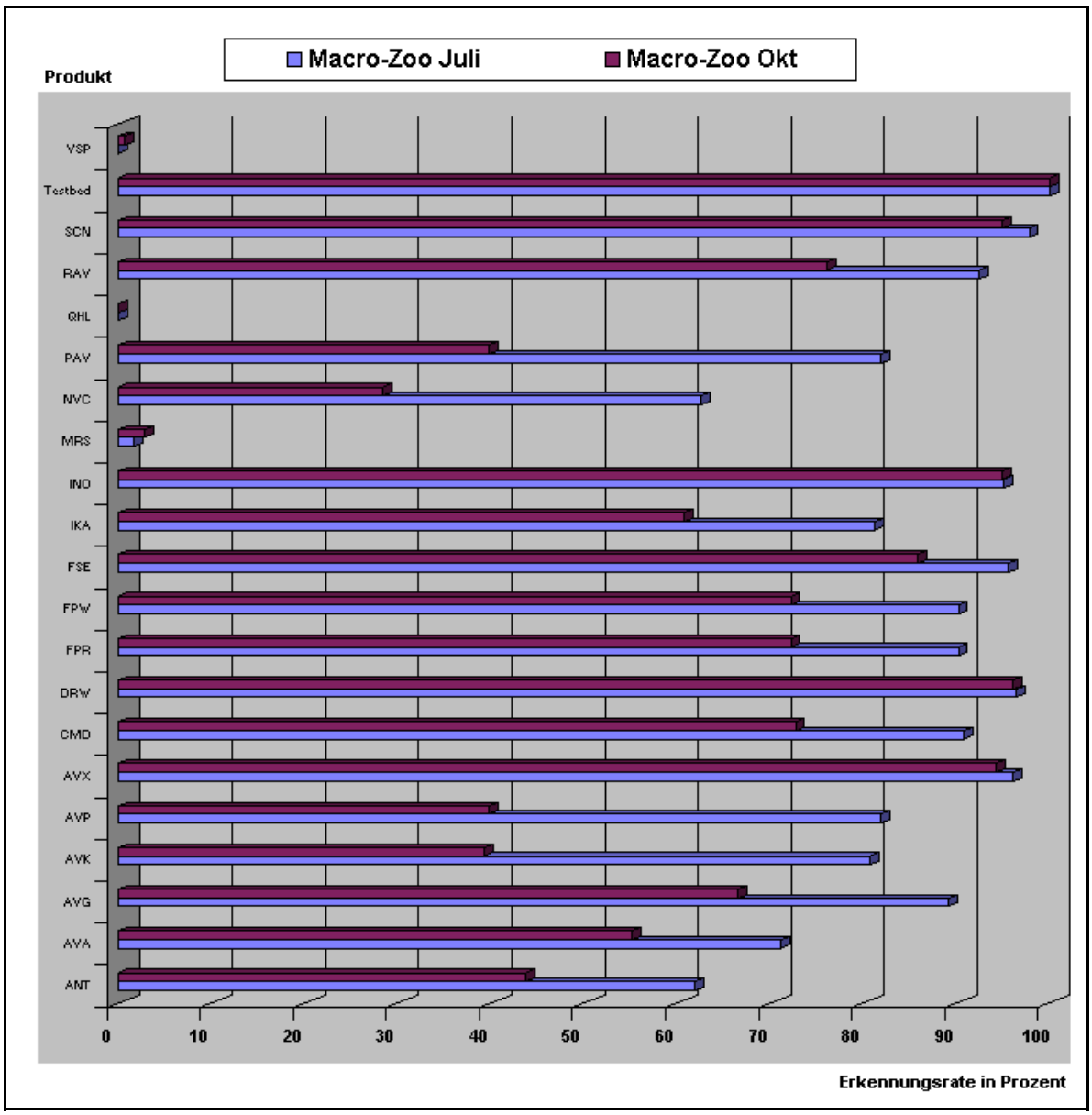

Abbildung 7.B: Entwicklung der Macro-Zoo Erkennung im Test 2002-03

Bei der Erkennung von Zoo-Viren (Abb. 7.B) ist überwiegend ein deutlicher Abfall der Erkennungsrate von Juli zu Oktober festzustellen. Neu erscheinende Zoo-Viren in den Monaten Juli bis Oktober können von den meisten Produkten nicht durch heuristische Verfahren entdeckt werden. Auch die Erkennung der Juli-Datenbank ist bei den meisten Produkten schlechter als im vorherigen VTC-Test (in welchem einige Produkte 100% Makro-Zoo-Erkennung erreicht hatten). Hierfür gilt das gleiche wie für den Abfall der Erkennung zwischen Juli und Oktober: neu erscheinende Zoo-Viren werden nicht erkannt.

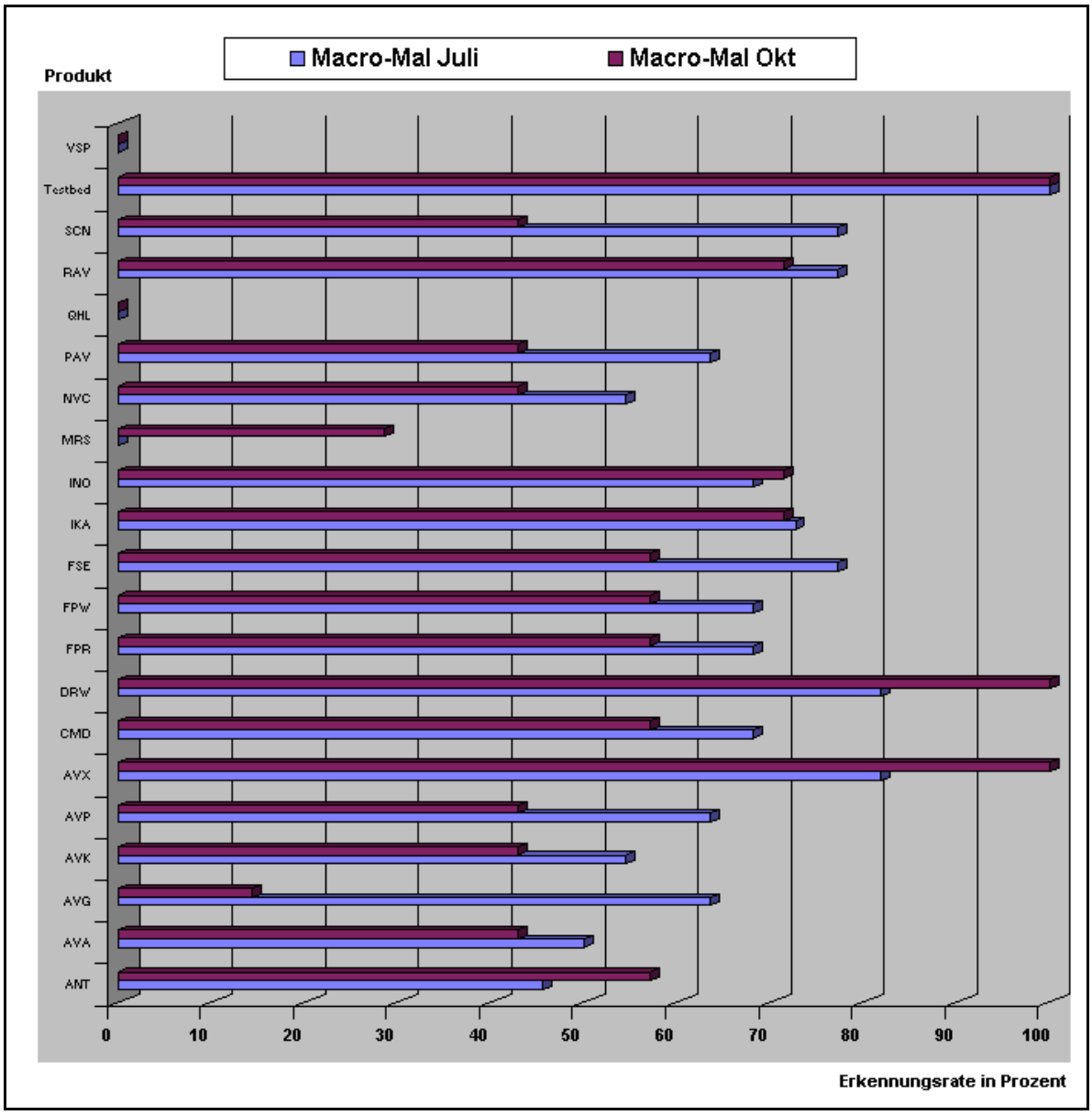

Abbildung 7.C: Entwicklung der Macro-Malware Erkennung im Test 2002-03

Die Erkennung von Makro-Malware (Abb. 7.C) ist auf geringerem Niveau als die Erkennung von Makro-Zoo-Viren. Auch hier nimmt die Erkennungsrate mit Alterung der Signatur (also von Juli zu Oktober) in der Regel ab. Ausnahmen sind die Produkte ANT, AVX und DRW, deren Erkennungsrate von Malware auf der Oktober-Datenbank deutlich höher ist als auf der Juli-Datenbank. Diese ungewöhnliche Steigerung der Erkennungsrate trotz Abnahme der Signaturaktualität kann nur durch gute heuristische Erkennungsverfahren der genannten Produkte erklärt werden. Dadurch erkennen die Produkte offensichtlich alle zwischen Juli und Oktober neu aufgetauchten Malwareobjekte. Es sei bemerkt, daß die Datenbank Makro-Malware-Oktober nur sieben maliziöse Objekte enthält, weshalb die Ergebnisse von geringer statistischer Relevanz sind und solche ungewöhnlichen Resultate entstehen können.

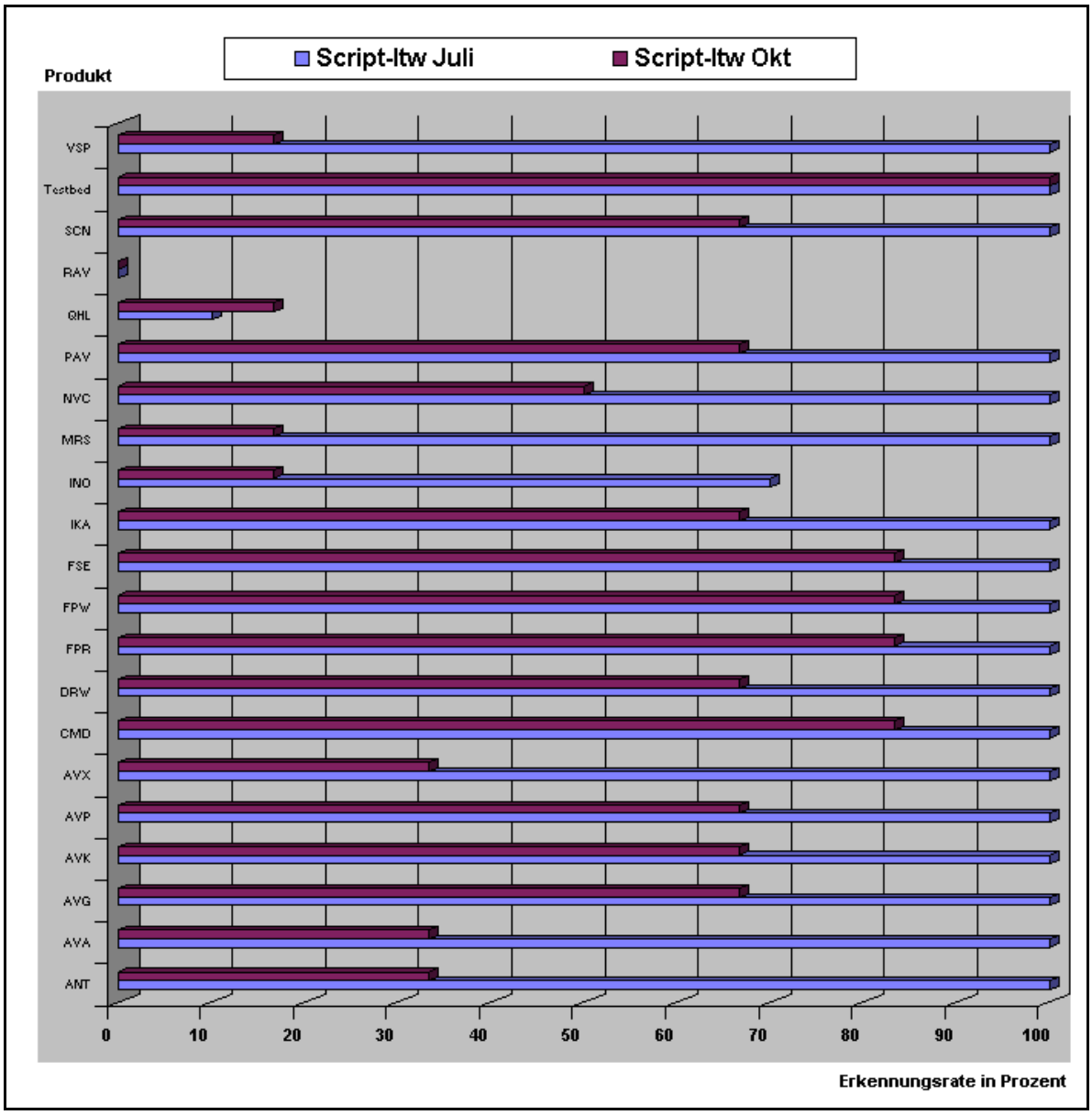

Abbildung 7.D: Entwicklung der Skript-Itw Erkennung im Test 2002-03

Die Erkennung von *in-the-wild* Skriptviren (Abb. 7.D) nimmt mit Abnahme der Signaturaktualität deutlich ab, wie die Diskrepanz zwischen der Erkennungsrate auf der Juli-Datenbank im Vergleich zur Oktober-Datenbank zeigt. Während Ende Juli noch fast alle Produkte mit Signatur von Mitte Juni 100 Prozent der Itw-Skriptviren erkennen, sinkt die Erkennungsrate zum Oktober bei allen Produkten deutlich. Diese Entwicklung ist unterschiedlich zur Erkennungsabnahme bei Itw-Makroviren (vgl. Abb. 7.A): die Itw-Skripterkennung sinkt stärker.

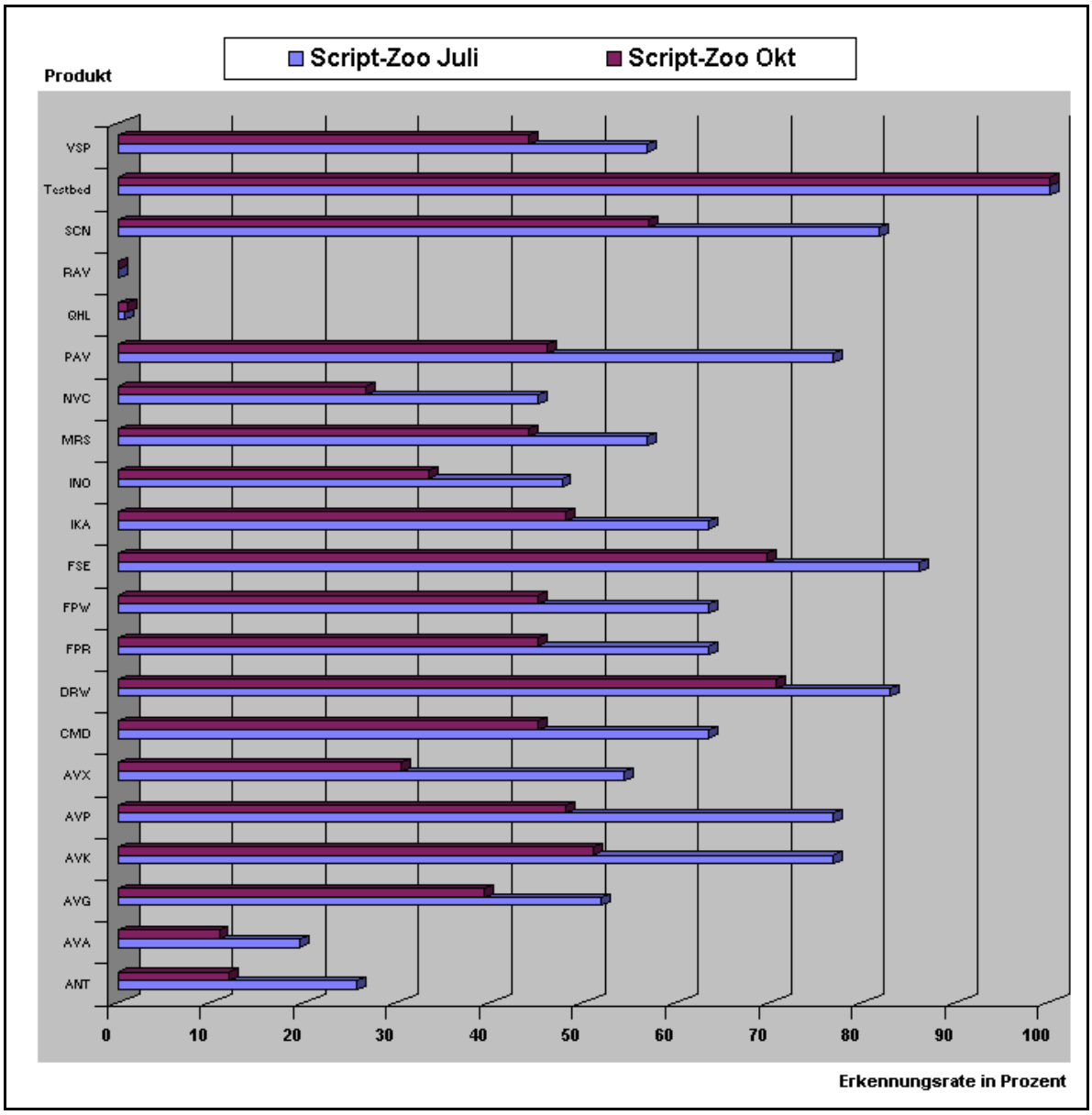

Abbildung 7.E: Entwicklung der Skript-Zoo Erkennung im Test 2002-03

Die Erkennung von Zoo-Skriptviren (Abb. 7.E) ist bereits im Juli bei fast allen Scannern (bis auf DRW, FSE und SCN) niedrig. Im Oktober ist sie bei allen Produkten inakzeptabel niedrig. Hier wird deutlich, daß in der Praxis ein regelmäßiges Signaturupdate für guten Schutz unabdingbar ist.

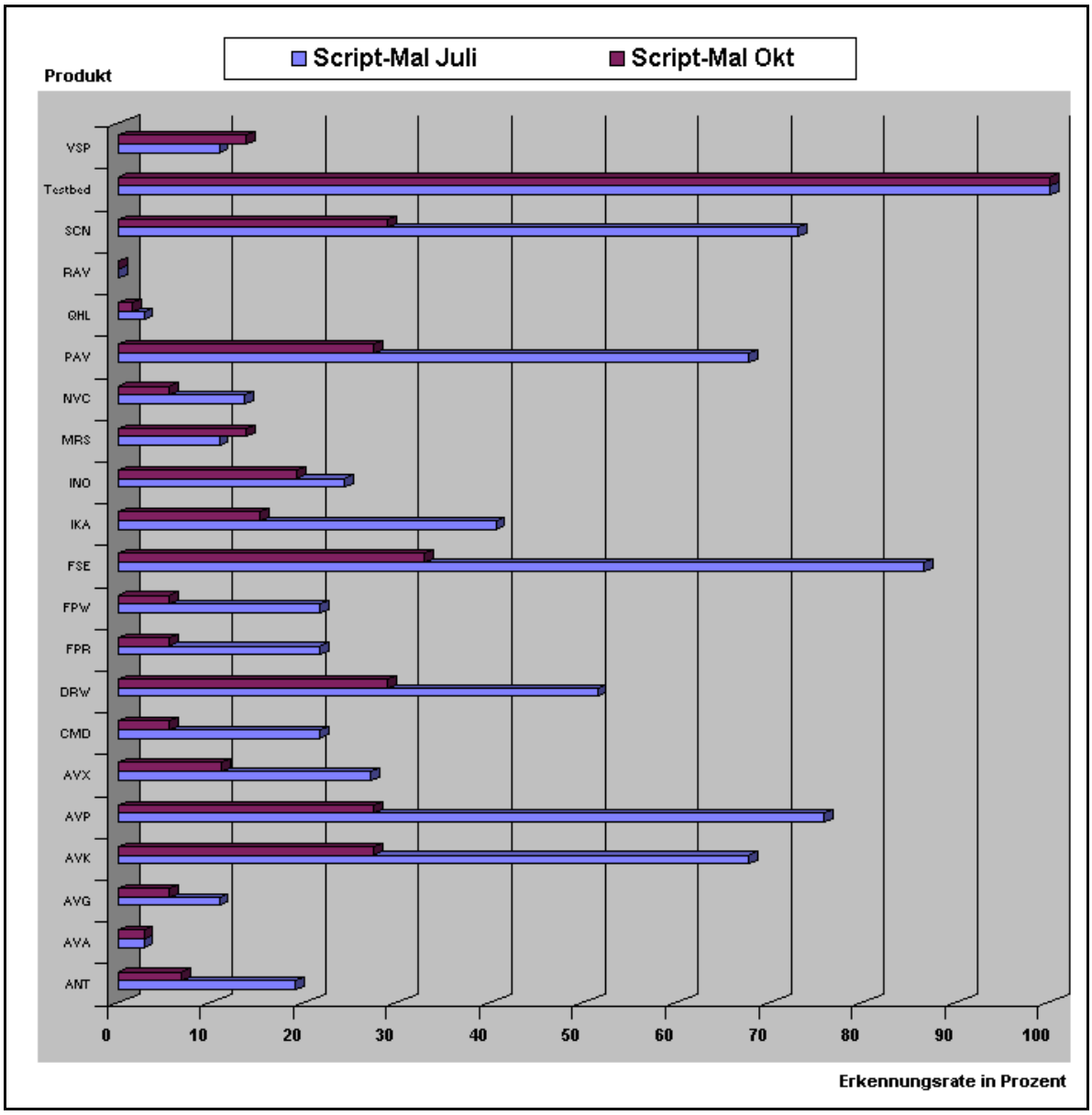

Abbildung 7.F: Entwicklung der Skript-Malware Erkennung im Test 2002-03

Bei Skript-Malware (Abb. 7.F) zeigt sich eine noch verheerende Entwicklung der Erkennungsrate als bei Skript-Zoo. Ohne Signaturupdates ist die Erkennungsrate hier bei allen Produkten Ende Oktober unter 35 %. Vor dieser Art von bösartiger Software ist der Benutzer ohne regelmäßige Signaturupdates bei sämtlichen Produkten im Test nur unzureichend geschützt.

7.2 Grafiken und Analysen zum Test 2001-10

Der Test 2001-10 ist einer der regelmäßig durchgeführten VTC-Tests, allerdings wurden in diesem Test keine File-Datenbanken (inklusive Poly und VKit) getestet (vgl. Abschnitt 4.3), sondern nur die Erkennung von Makro- und Skript-Malware. Es werden folgende durch die Datenbank VTED aufbereitete Testergebnisse betrachtet:

- Abweichung der Windows32-Erkennung (7.2.1)
- Ergebnisgrafiken für Makro- und Skripterkennung (7.2.2)

7.2.1 Windows32-Abweichungen der Erkennungsrate

Eine interessante Analyse der VTC-Testergebnisse ist der Vergleich der Produkte hinsichtlich ihres Verhaltens unter den drei getesteten Windows32-Betriebssystemen[94]. Da diese Betriebssysteme ähnliche Plattformen darstellen und viele Hersteller nur ein Produkt für alle Windows32-Betriebssysteme entwickeln, ist der Vergleich der Erkennungsrate pro Datenbank unter den drei Betriebssystemen eine interessante Analyse. Bei gleichen Erkennungsraten aller getesteten Produkte könnte sogar in zukünftigen Tests nur noch ein Windows32-Referenzsystem getestet werden, da die Produkte die gleichen Ergebnisse auf den anderen Windows32-Betriebssystemen nachweisbar geliefert hätten und man so die Erkennung als konsistent voraussetzen könnte.

Tabelle 7.G zeigt die Produkte und Datenbanken, bei denen im Test 2001-10 Abweichungen der Erkennungsrate unter Windows32-Betriebssystemen festzustellen waren. Es wird zusätzlich pro Scanner die maximale Abweichung (in Prozent) aller Windows32-Ergebnisse einer Datenbank angegeben.[95]

[94] Windows98, WindowsNT und Windows2000

[95] In der ersten Zeile bedeutet zum Beispiel die 0,79% als maximale Abweichung von ANT unter Macro-Mal, daß die Erkennungsraten dieses Produktes unter der Datenbank Macro-Mal maximal 0,79% voneinander abweichen.

Abkürzung	Datenbank	Max-Abweichung in Prozent
ANT	Macro-Mal	0,79%
ANT	Macro-Zoo	0,32%
AVA	Macro-Mal	0,53%
AVA	Macro-Zoo	0,02%
AVA	Script-Zoo	12,12%
AVX	Macro-Pack	4,90%
AVX	Macro-Pack-ARJ	4,90%
AVX	Macro-Pack-CAB	4,90%
AVX	Macro-Pack-LHA	4,90%
AVX	Macro-Pack-RAR	4,90%
AVX	Macro-Pack-WRAR	4,90%
AVX	Macro-Pack-ZIP	4,90%
CMD	Script-Itw	5,26%
CMD	Script-Zoo	0,72%
FPR	Script-Zoo	0,36%
INO	Macro-Mal	1,26%
INO	Script-Zoo	1,25%
NAV	Macro-Zoo	0,07%
RAV	Macro-Mal	0,24%
RAV	Script-Zoo	99,79%

Tabelle 7.G: Auflistung aller Abweichungen der Erkennungsrate unter Windows32-Betriebssystemen im Test 2001-10

Tabelle 7.H verdichtet diese Daten zu einer Zeile pro Testprodukt, in der die maximale Abweichung der Erkennung unter allen Malware-Datenbanken dargestellt wird. Somit liefert Tabelle 7.H eine Gesamtübersicht über das konsistente Erkennungsverhalten der Testprodukte im Test 2001-10. Es zeigt sich, daß bis auf wenige Ausnahmen (AVA, CMD und RAV) die Produkte unter allen Windows32-Betriebssystemen gleiche oder nur geringfügig[96] abweichende Ergebnisse geliefert haben.

Dennoch deuten die Ergebnisse der Windows32-Abweichungen nicht daraufhin, daß die Erkennungsraten der Testprodukte unter diesen Betriebssystemen generell als gleich erachtet werden können und somit der Test eines Windows-Betriebssystem ausreichen würde. Durch die in der Datenbank VTED integrierten, automatischen Abfragen zur Analyse der Windows32-Abweichungen lassen sich diese Annahmen allerdings regelmäßig nach Durchführung eines Tests erneut überprüfen.

[96] unter 5%

Abkürzung	Max von Max-Abweichung in Prozent
ANT	0,79%
AVA	12,12%
AVG	0,00%
AVK	0,00%
AVP	0,00%
AVX	4,90%
CMD	5,26%
DRA	0,00%
DRW	0,00%
DSE	0,00%
FPW	0,00%
FSE	0,00%
FPR	0,36%
IKA	0,00%
INO	1,26%
NAV	0,07%
NVC	0,00%
PAV	0,00%
QHL	0,00%
RAV	99,79%
SCN	0,00%
Testbed	0,00%
VSP	0,00%

Tabelle 7.H: Auflistung der maximalen Abweichung der Erkennungsrate pro getestetem Produkt unter Windows32-Betriebssystemen im Test 2001-10

7.2.2 Ergebnisgrafiken

Zur übersichtlichen Betrachtung der Testergebnisse unter den einzelnen Betriebssystemen werden für folgende Betriebssysteme jeweils die Ergebnisse der Erkennungsrate von Makro- und Skript-Malware grafisch dargestellt:

- Windows NT[97]
- DOS
- Linux

[97]Da sich die Erkennungsraten unter den verschiedenen Windows32-Betriebssystemen bei den meisten Produkten nur gering unterscheiden (vgl. 7.2.1), soll an dieser Stelle lediglich Windows NT als Referenzsystem für die Erkennung von Malware unter Windows-Systemen betrachtet werden. Ergebnisse zu Windows 98 und Windows 2000 finden sich auf der VTC-Webseite, auch in grafischer Darstellung (siehe [VTC 2001-10a]).

Mit Windows NT wird nur ein einziges Windows32-Betriebssystem betrachtet. Die Grafiken zeigen für jedes getestete Produkt jeweils die Erkennungsrate von Itw-Viren, Zoo-Viren, und nichtviraler Malware (als Datenbank *Malware* bezeichnet). Durch die grafische Darstellung wird auch ein Vergleich der Erkennungsrate eines Produktes auf einer bestimmten Datenbank zu den Ergebnissen anderer Testteilnehmer erleichtert.

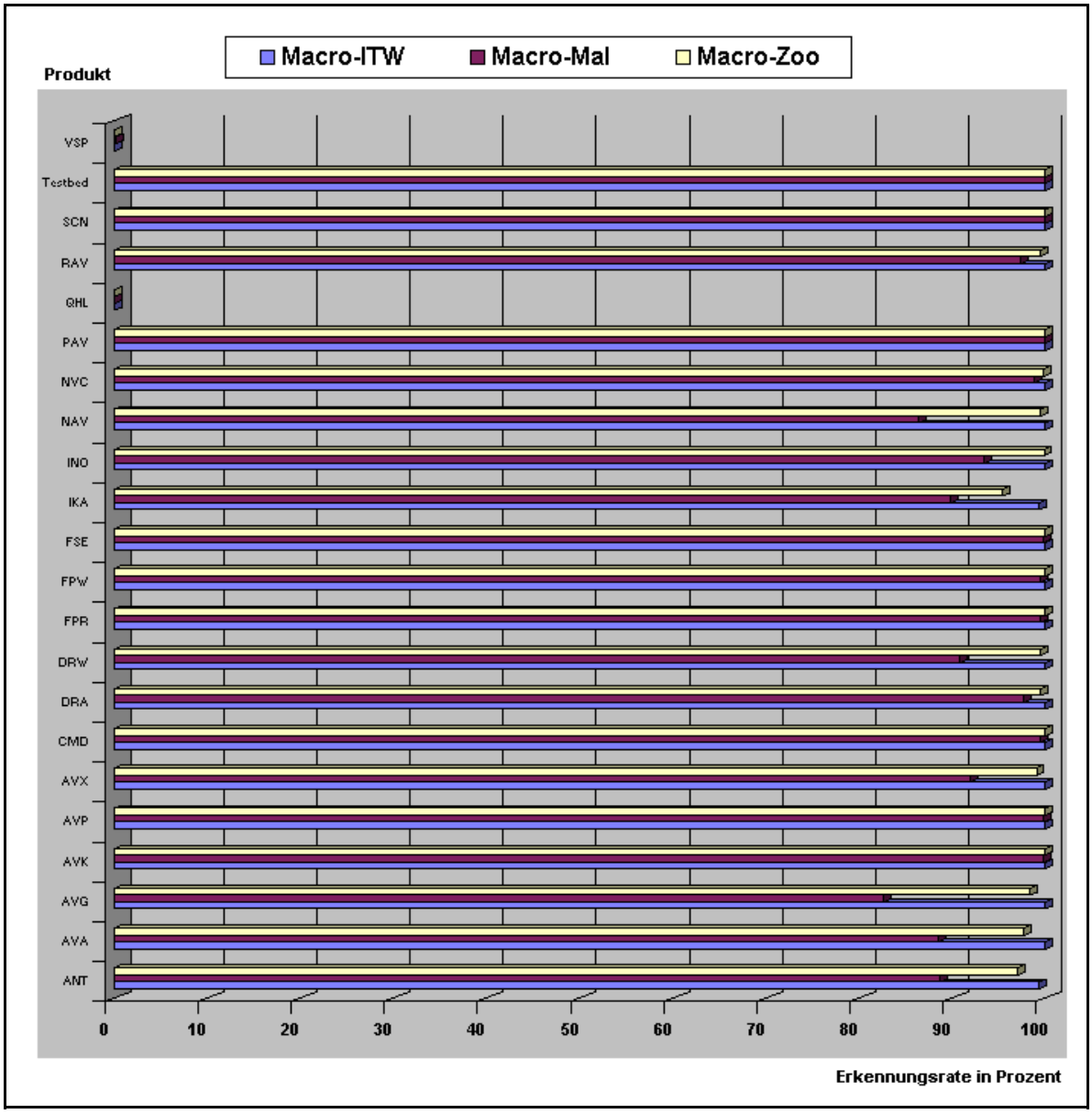

Abbildung 7.I: Erkennung von Makro-Malware im Test 2001-10 unter Windows NT

Abbildung 7.I zeigt die Erkennung von Makro-Malware unter Windows NT. Makroviren, die verbreitet sind (*in-the-wild*), werden von fast allen Produkten im Test sehr gut erkannt (Ausnahme: VSP und QHL). Die Zoo-Erkennung ist ähnlich gut, hier zeigen sich jedoch

geringe Schwächen einiger Scanner. Die Erkennung von Makro-Malware ist bei einigen Produkten ungenügend. Insgesamt besteht bei vielen Produkten ein ausreichend guter Schutz für den Benutzer vor bösartiger Makro-Software.

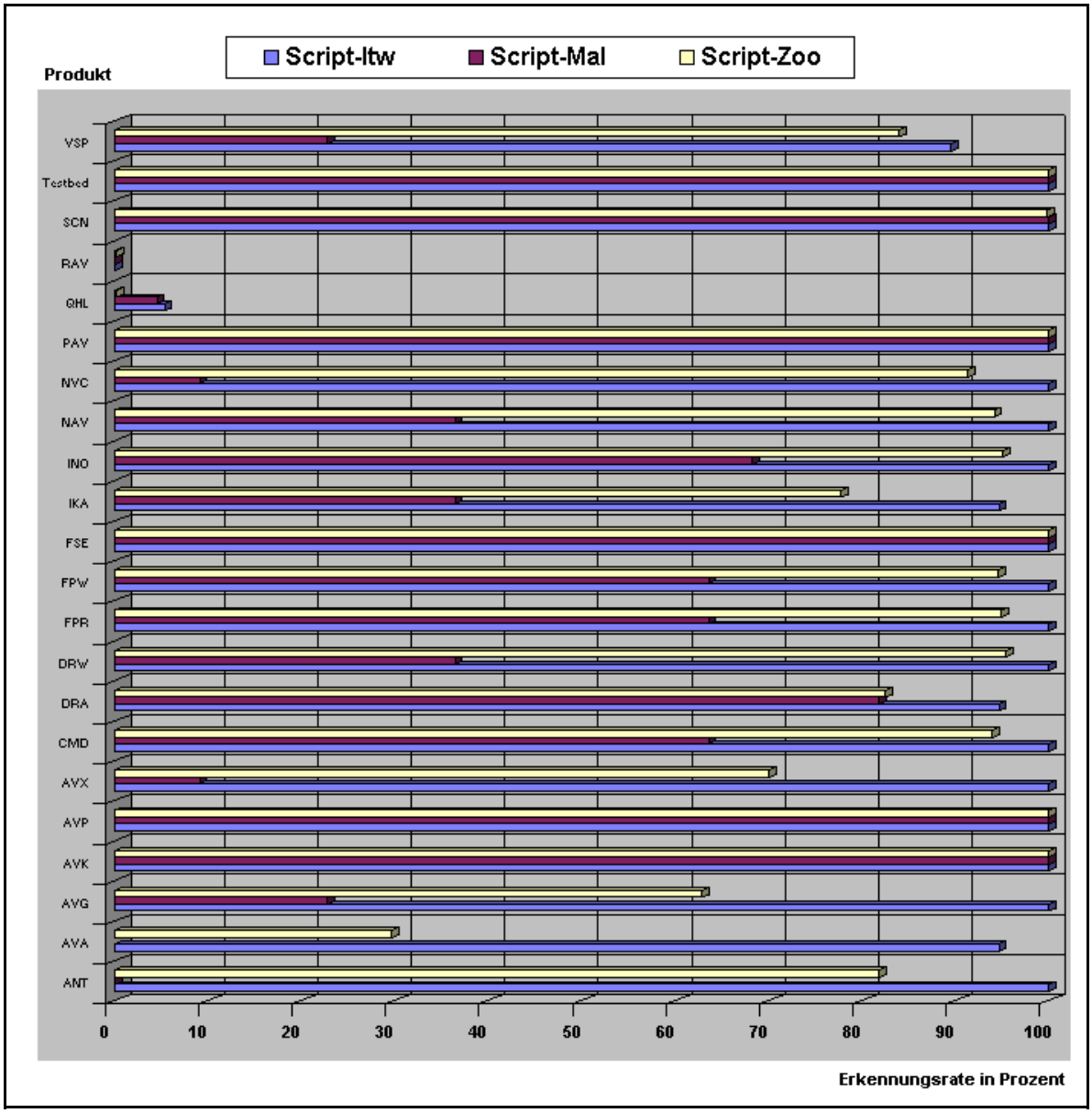

Abbildung 7.J: Erkennung von Skript-Malware im Test 2001-10 unter Windows NT

Bei der Erkennung von Skript-Malware (Abb. 7.J), werden Unterschiede zwischen den einzelnen Produkten im Test deutlich. Nur wenige Produkte haben eine perfekte Erkennungsrate sowohl bei *in-the-wild*- und Zoo-Viren als auch bei Skript-Malware (AVK, AVP, FSE, PAV und SCN). Die Erkennung von Zoo-Viren und Malware ist bei vielen Produkten ungenügend und stellt einen unzureichenden Schutz für die Benutzer der entsprechenden Produkte dar.

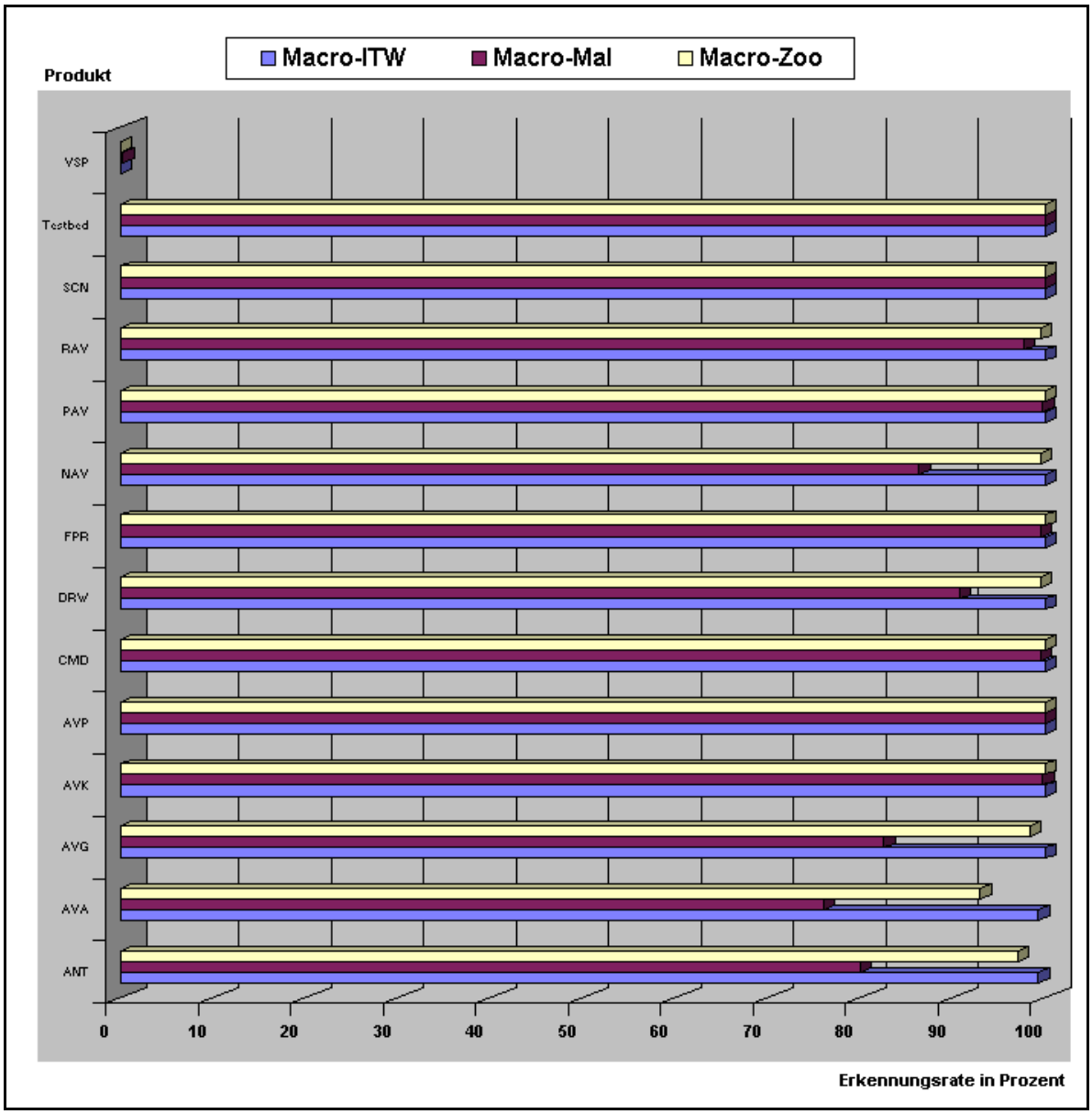

Abbildung 7.K: Erkennung von Makro-Malware im Test 2001-10 unter DOS

Abbildung 7.K zeigt die Erkennung von Makro-Malware unter DOS. Für das Betriebssystem DOS haben weniger Hersteller Produkte für den Test 2001-10 eingereicht als für Windows NT. Dies liegt daran, das dieses Betriebssystem nicht mehr so verbreitet im Einsatz ist und deshalb nicht alle Hersteller Produkte für DOS liefern. Für die Erkennung von Makroviren zeigen sich ähnliche Resultate wie unter Windows NT: *in-the-wild* Makro-Viren werden von fast allen Produkten im Test sehr gut erkannt (Ausnahme: VSP), die Erkennungsraten von Zoo-Viren und nichtviraler Malware (Datenbank *Macro-Mal*) fallen teilweise ab. Insgesamt besteht bei vielen Produkten ein ausreichend guter Schutz für den Benutzer vor bösartiger Makro-Software.

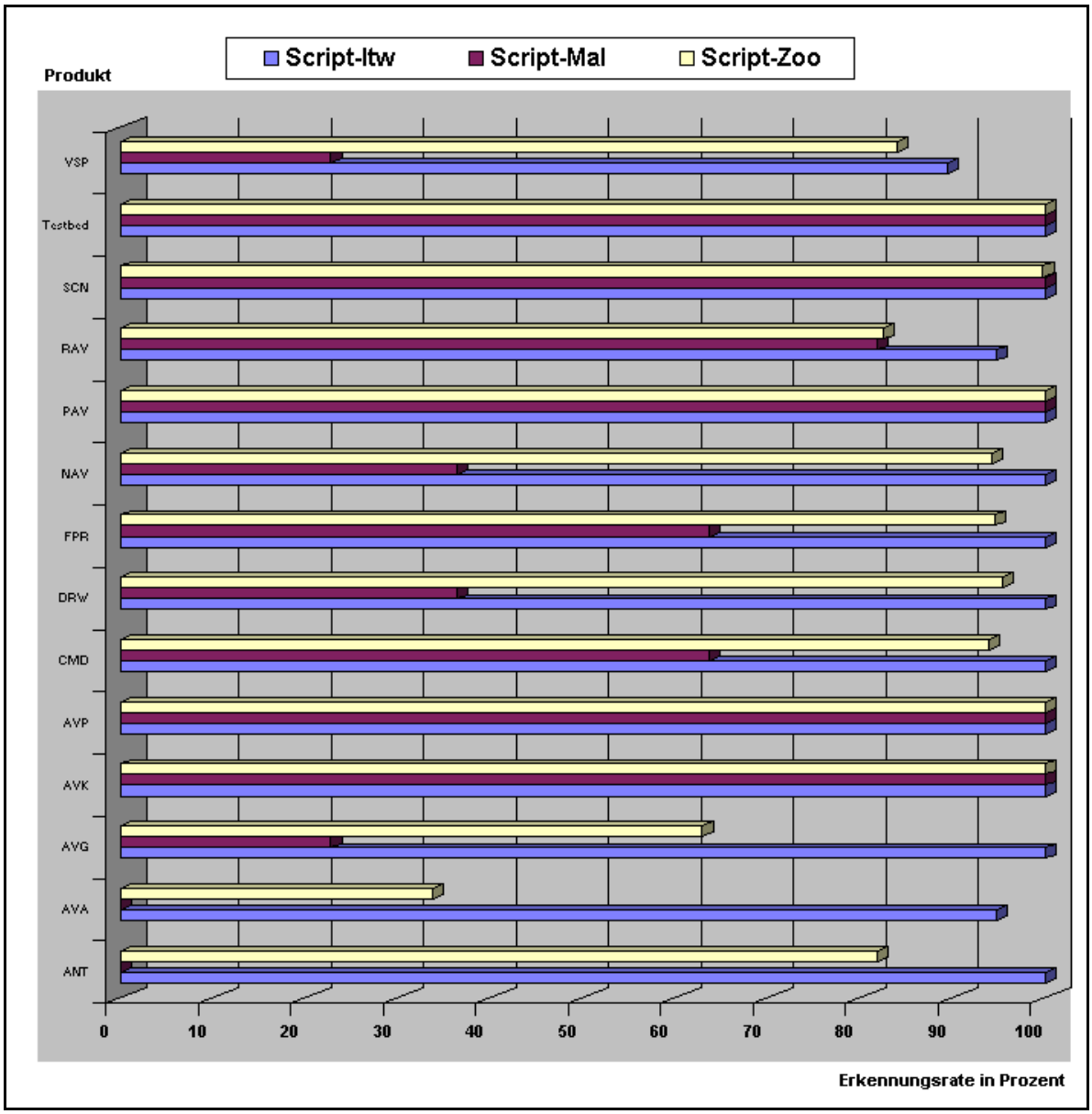

Abbildung 7.L: Erkennung von Skript-Malware im Test 2001-10 unter DOS

Die Erkennungsraten von Skript-Malware im VTC-Test 2001-10 unter DOS (Abb. 7.L) sind nur bei vier Produkten im Test sehr gut: AVK, AVP, PAV und SCN. Alle anderen Testprodukte zeigen bei der Erkennung von Skriptviren und -malware erhebliche Schwächen. Insbesondere die Erkennungsraten von nichtviraler Skriptmalware (Datenbank *Script-Mal*) sind außer bei den genannten vier Testprodukten sehr niedrig, bei zwei Produkten (ANT und AVA) ist die Erkennungsrate in diesem Bereich sogar bei 0%. Lediglich bei Skriptviren, die als *in-the-wild* eingestuft werden, zeigen einige der anderen Scanner gute Ergebnisse (Erkennungsrate über 90%).

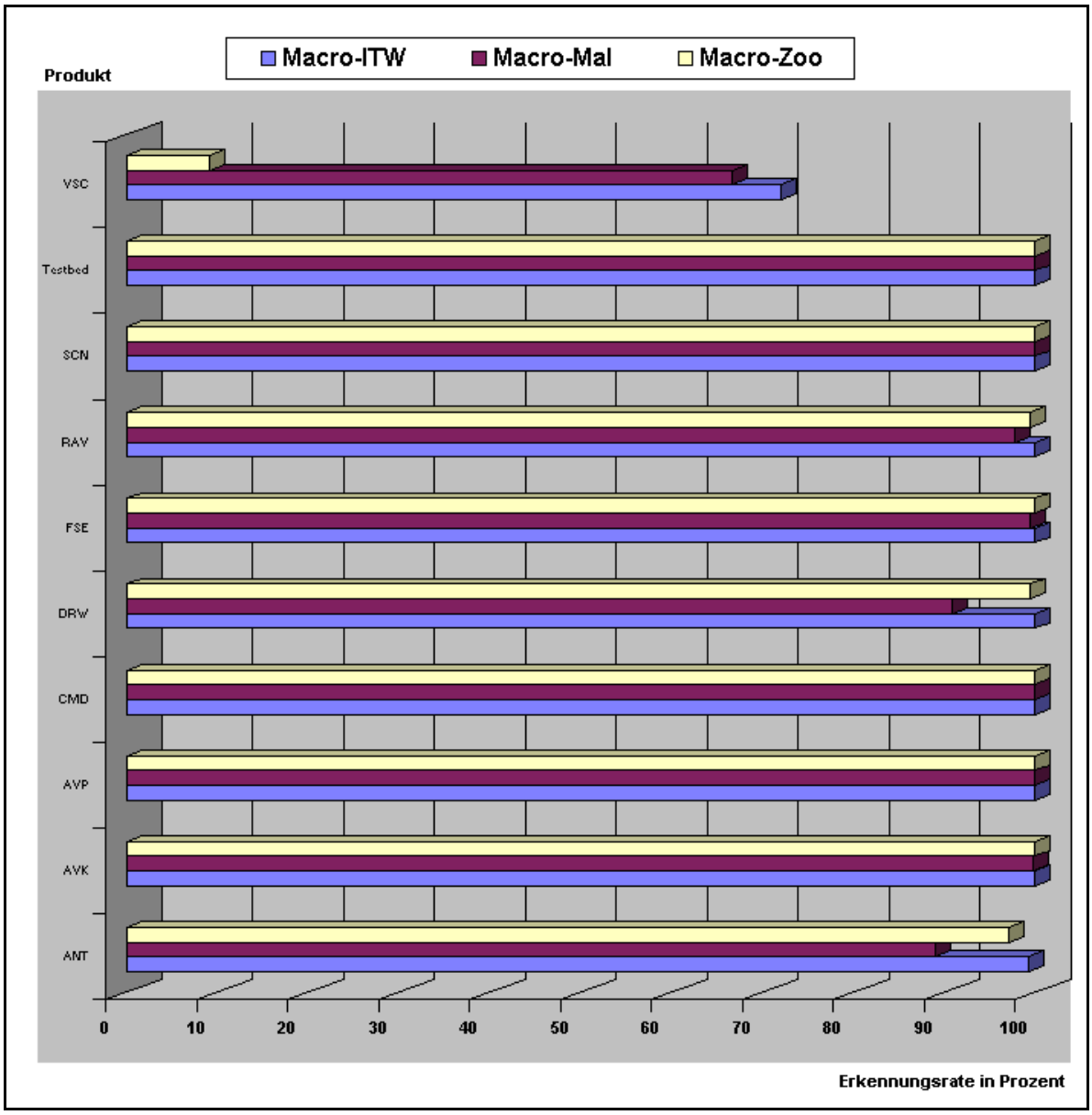

Abbildung 7.M: Erkennung von Makro-Malware im Test 2001-10 unter Linux

Unter Linux haben nur wenige Hersteller Testprodukte für den Test 2001-10 eingereicht (9 Produkte). Allerdings zeigen die für Linux eingereichten Produkte auf den Makro-Datenbanken gute bis sehr gute Ergebnisse. ANT und DRW fallen durch niedrige Erkennungsraten unter *Makro-Mal* auf. Einzig die Erkennung von VSC ist ungenügend.

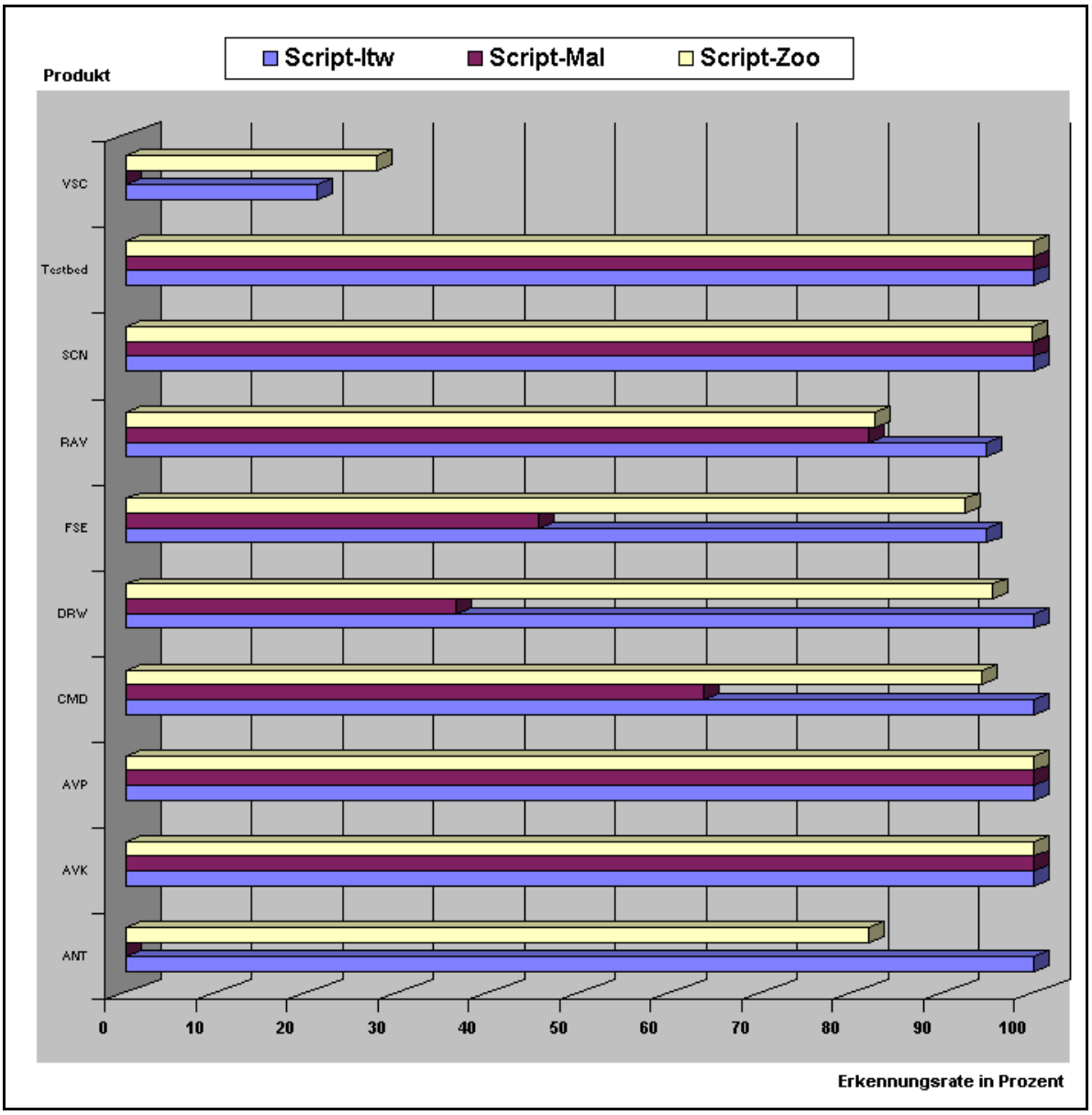

Abbildung 7.N: Erkennung von Skript-Malware im Test 2001-10 unter Linux

Bei der Erkennung von Skript-Malware (Abb. 7.N) unter Linux zeigen sich - im Gegensatz zur Erkennung von Makro-Malware - deutliche Unterschiede zwischen den Testprodukten. Drei Produkte können auf allen drei Skript-Datenbanken eine Erkennungsrate von 100% vorweisen: AVK, AVP und SCN. Bei den anderen Produkten sind insbesondere die Erkennung von Skript-Zoo-Viren und nichtviraler Skript-Malware nicht ausreichend.

7.3 Betrachtungen und Grafiken von Testergebnissen mehrerer Tests

Einer der Vorteile der Integration von Testergebnissen in eine Datenbank ist die Möglichkeit der vergleichenden Darstellung von Testergebnissen mehrerer Tests. Solche Darstellungen - auch als Zeitreihen bezeichnet - betrachten die langfristige Entwicklung und sollen in den folgenden beiden Unterabschnitten für einige Datenbanken aufgezeigt werden. Die Zeitreihen werden dabei als Tabelle mit den Erkennungsraten jedes Produktes pro Test (7.3.1) oder als Grafiken mit den jeweiligen Durchschnittswerten aller Produkte pro Datenbank und Test (7.3.2) dargestellt.

7.3.1 Tabellen von Zeitreihen

In tabellarischer Darstellung wird für jeden Test als Spalte und jedes Testprodukt als Zeile in der korrespondierenden Zelle die entsprechende Erkennungsrate des jeweiligen Produktes im jeweiligen Test angegeben. So wird die Entwicklung der Erkennungsrate pro Testprodukt in den durchgeführten Tests deutlich. Eine leere Zelle bedeutet, daß das entsprechende Produkt (Zeile) an dem Test (Spalte) nicht teilgenommen hat.

Für die Zoo-Datenbanken werden bereits in jedem VTC-Testbericht die Zeitreihen mit der Erkennungsrate pro getestetem Scanner und Test angegeben. Deshalb werden in diesem Abschnitt die Zeitreihen für die Malware-Datenbanken (sowohl File-Mal als auch Makro-Mal), also die Erkennung von nichtviraler Malware in den VTC-Tests seit 1997, angegeben. Tabelle 7.O zeigt die Zeitreihe aller Produkte für die Erkennungsrate von File-Malware unter DOS. Tabelle 7.P zeigt die Zeitreihe aller Produkte für die Erkennungsrate von Makro-Malware unter DOS.

Die tabellarischen Zeitreihen sind für das Betriebssystem DOS aufgelistet, weil dieses Betriebssystem am längsten in VTC-Tests getestet wird und somit die Entwicklung der Erkennungsrate der Produkte am besten verdeutlichen kann. Durch die Datenbank VTED lassen sich aber auch für alle anderen getesteten Betriebssysteme entsprechende Zeitreihen für sämtliche Datenbanken erzeugen. Weitere Zeitreihen unter DOS, die ebenfalls bisher nicht in VTC-Testberichten veröffenlicht wurden, finden sich in Anhang C[98].

[98]In Anhang C werden Zeitreihen für VKit, Poly, File-Itw, Makro-Itw, Skript-Itw, Boot-Zoo und Boot-Itw unter DOS angegeben.

Abkürzung	1997-07	1998-02	1998-10	1999-03	1999-09	2000-04	2001-04
al4	25,2	70,4					
ANT		85,4	52,7				
AVA				66,5	60,6	56,5	51
AVE	77,9						
AVG	25,2		71,2	65,3	57		50,6
AVK			93,6	94,8			96
AVP	85,3	86,4	94,5	88,3	85,9	83,2	96,4
AVS	27		80,2				
CMD					83,7	92,8	
DRW	25,2	65,1	79,5	74,6			
dsa	100						
DSS		98,1	98,4	97,5			
FPR	47,2	86,4		89,2	84,8	95,3	94
FSE			94,5	88,7	84,3	94,6	
IBM	15,3						
IMS	12,9						
INO		90,1	86,7	75,3	82,3	74,7	47,9
IRI		48,6					
IRS				43,5			
ITM		42,4	46,7	44,8			
MR2					43,5		41,9
NAV	24,5			76,8	62,6	73,4	45,1
NOD				63,4	64,6	77,6	
NVC	36,8	71,5	72,7	69,4		64,9	
PAN		59,3					
PAV	74,8	87		94,8	84,5	90,8	96,2
PRO				12			
RAV			63,7				
SCN	34,4	79,3		97,2	96,1	93,4	90,4
SWP	50,9				76,8	78,3	
TBA	35	68,2	61,8				
TSC		41	67,9	57,2	41,6		
vb4	12,9						
VDS	7,4	29,9					
VET	15,3			43,8			
VIT						6,3	
VSA		47,1					
VSP			66,8	69,3	58,1	50,5	43,7
VSW		48,6					

Tabelle 7.O: Zeitreihen für File-Malware unter DOS in VTC-Tests seit 1997

Abkürzung	1997-02	1997-07	1998-02	1998-10	1999-03	1999-09	2000-04	2000-08	2001-04	2001-10
al4	60	34	27,8							
ANT			77,8	23,4			67,3	78,4		80
AS7		88								
AVA					91,5	85,6	80,8		79,4	76,1
AVE		82								
AVG	33,3	46		69,4	69	82			80,1	82,6
AVK				96,4	95,8			98,2	99,3	99,8
AVP	86,7	88	95,8	96,4	95,8	99,4	96,9		99,3	100
AVS	53,3	44		93,7						
CMD						98,8	100	100		99,5
DRW	60	60	77,8	91	81,7	84,4	78,5	69,8	83,1	90,8
dsa	86,7	86								
DSS			98,6	100	98,6					
FMA	46,7	86								
FPR	6,7	2	97,2		97,9	98,8	100	100	99,8	99,5
FSE				96,4	95,8	94,6	96,2			
FWI	53,3									
FWN		86	84,7							
HMV			86,1	89,2	96,5					
IBM	26,7	46								
IMS		22								
INO			83,3	93,7	95,8	96,4	95	92,8	90,6	
IRI			4,2							
IRS					53,5					
ITM	53,3		26,4	31,5	27,5					
MR2						67,1			34,5	31,7
NAV	66,7	76			90,8	94	81,5	76,6	72,2	86,4
NOD					96,5	100	96,2			
NVC	13,3	88	88,9	88,3	90,1	91	95,4	99,4	99	
PAN			56,9							
PAV		76	95,8		94,4	96,4	98,8		99,3	99,8
PCC		38								
PRO					59,2	17,4				
RAV				96,4	81,7					97,7
SCN	60	78	93,1		97,9	100	99,6	98,8	99,8	100
SWP	53,3	56				94	95			
TBA	46,7	84	88,9	91,9						
TNT	20									
TSC			75	9,6	73,9	67,1				
UKV								3		
VDS	6,7	4	1,4							
VET		80	87,5	82,9	89,4					
VIT	6,7						1,9			
VRX	0									
VSA			72,2							
VSP						0,6	0,4		0,2	0,2
VSW			72,2							

Tabelle 7.P: Zeitreihen für Makro-Malware unter DOS in VTC-Tests seit 1997

7.3.2 Grafiken von Zeitreihen

In der grafischen Darstellung von Zeitreihen, die durch die Datenbank VTED erstellt werden, wird im Unterschied zur tabellarischen Darstellung nur der Durchschnittswert der Erkennungsrate des jeweiligen Tests und der jeweiligen Datenbank ausgegeben. Dies ergibt eine Übersicht der Gesamtentwicklung der Erkennung von Test zu Test. Dementsprechend eignen sich die Grafiken zur Betrachtung der Verbesserung von Anti-Viren-Technik insgesamt (als Durchschnitt aller getesteten Produkte).

Die Abbildungen 7.Q bis 7.T zeigen die Entwicklung der durchschnittlichen Erkennungsrate unter DOS, da dieses Betriebssystem am längsten in VTC-Tests getestet wird[99]. Zeitreihen mit Durchschnittswerten anderer Betriebssysteme können durch die Datenbank VTED ebenfalls erstellt werden.

Die durchschnittliche Erkennungsrate gibt einen Anhaltspunkt über den Schutz der Benutzer zum jeweiligen Testzeitpunkt[100]. Da die Produkte unterschiedlich stark verbreitet sind, würde eine Gewichtung der Erkennungsrate mit dem Marktanteil pro Produkt eine exaktere Angabe über den tatsächlichen durchschnittlichen Schutz der Benutzer ermöglichen. Dennoch zeigen die Grafiken tendenzielle Entwicklungen auf. In allen vier Grafiken erkennt man langfristig (durch leichte Schwankungen unterbrochen) eine Steigerung der durchschnittlichen Erkennungsrate pro Datenbank. Hat die durchschnittliche Erkennungsrate einen gewissen Wert erreicht, schwankt sie bei vielen Datenbanken nur noch in geringem Maße. Besonders bei den Datenbanken nichtviraler Malware (File-Mal in Abb. 7.Q und Makro-Mal in Abb. 7.R) wird die positive Entwicklung der Anti-Malware-Erkennung von 1997 bis 2001 deutlich. Dennoch ist die Erkennung bei beiden Datenbanken mit durchschnittlich unter 90 Prozent noch steigerungsfähig. Anti-Malware-Produkte bieten den Benutzern gegenüber nichtviraler Malware 2001 im Durchschnitt einen besseren Schutz als 1997.[101]

Einige Schwankungen der durchschnittlichen Erkennungsrate (wie zum Beispiel in Grafik 7.R zwischen 2000-04 und 2001-04 bei Mac-Itw und Mac-Zoo) sind dadurch bedingt, daß die Anzahl der Testprodukte über die verschiedenen Tests variiert. Dementsprechend ändert sich das arithmetische Mittel: bei Tests mit sehr vielen Testprodukten sind hohe Durchschnittswerte nur bei durchweg guten Produkten zu erreichen.

---

[99] Die Punkte geben jeweils den Durchschnitt der tatsächlich im Test gemessenen Erkennungsrate wieder, die Verbindungslinien zwischen den Punkten approximieren linear die durchschnittliche Erkennungsrate zwischen den Tests.

[100] genauer: zum Zeitpunkt des Einreichens der Testprodukte (*submission deadline*)

[101] Diese Aussage wird durch die angesprochene unterschiedliche Verbreitung der Produkte nicht relativiert, da eher die am Markt nicht verbreiteten Produkte den Durchschnittswert der Erkennung durch schlechte Ergebnisse vermindern. Der tatsächliche durchschnittliche Schutz der Produkte liegt also durch unterschiedlich hohe Benutzerzahlen pro Produkt noch höher als in den Grafiken ersichtlich.