KES/KPMG-Sicherheitsstudie 2002

Kapitel 5: Sonstige ISi-Maßnahmen

UIMC Dr. Vossbein Gmbh & Co KG, Wuppertal

5.01

Welche der folgenden Maßnahmen sind in Ihrem Haus realisiert/geplant?												
	Server				Clients				mobile Endgeräte (Notebooks, PDAs)			
	realisiert	geplant	nicht vorgesehen	Summe	realisiert	geplant	nicht vorgesehen	Summe	realisiert	geplant	nicht vorgesehen	Summe
Firewalls	237	4	1	242	81	5	54	140	53	5	52	110
Virenschutzmechanismen	247	2	4	253	245	4	4	253	202	13	14	229
Intrusion Detection System	77	79	23	179	11	29	53	93	4	24	53	81
Benutzerverzeichnis mit Security-Policy	129	41	17	187	78	23	26	127	65	18	27	110
Authentisierung	229	61	37	234	234	75	37	242	218	61	37	229
- Hardware Token	27	18	28	73	32	20	31	83	46	16	31	93
- Passwort	225	0	5	230	222	1	8	231	200	4	9	213
- Chipkarte	7	40	30	77	21	54	30	105	18	41	32	91
- biometrische Verfahren	3	22	35	60	2	25	35	62	0	15	36	51
Protokollierung unberechtigter Zugriffe	199	26	3	228	84	8	25	117	77	4	27	108
Content Inspection/Filtering (Adress-/Inhaltsfilter)	96	29	21	146	25	22	32	79	21	13	34	68
Proxy-Server	195	12	8	215	70	7	27	104	52	9	30	91
Public Key Infrastructure (PKI)	28	87	23	138	27	65	27	119	18	52	32	102
Verschlüsselung	147	117	36	209	132	101	36	197	134	120	36	199
- sensitive Dateien	79	61	20	160	67	42	17	126	92	49	18	159
- Festplatten (kpl.)	24	45	26	95	22	40	28	90	61	69	18	148
- Archivdatenträger/Backups	35	21	24	80	16	21	27	64	15	17	26	58
- LAN / Intranet-Verbindungen	58	39	21	118	53	28	25	106	43	36	27	106

- WAN / Internet-Verbindungen	86	49	15	150	73	26	20	119	59	25	25	109
- Telefon	15	11	33	59	10	6	33	49	5	9	35	49
- Fax	10	7	35	52	11	2	35	48	8	5	36	49
- E-Mail	68	67	20	155	79	58	18	155	62	61	21	144
Physische Sicherheit	253	76	33	256	144	45	36	170	90	40	36	137
- Zutrittskontrolle	218	13	7	238	95	10	22	127	41	7	28	76
- Bewachung	117	12	20	149	50	5	30	85	19	2	33	54
- Video-Überwachung	71	18	28	117	14	8	33	55	1	5	35	41
- Einbruchsmeldesysteme	178	9	10	197	69	4	27	100	24	3	31	58
- Schutz von Glasflächen gegen Durchbruch / Durchwurf	141	10	19	170	37	0	32	69	7	0	36	43
- Sicherheitstüren	192	17	8	217	46	7	28	81	18	3	33	54
- Brandmeldesysteme	209	9	7	225	87	1	21	109	28	0	32	60
- Löschanlagen	126	22	16	164	32	6	33	71	7	3	36	46
- andere Meldesystem (z. B. Gas, Staub, Wasser)	97	9	26	132	12	0	34	46	4	3	35	42
- Datensicherungsschränke/-räume	202	8	8	218	46	5	28	79	23	0	30	53
- Schutz gegen kompromittierend Abstrahlung	32	7	31	70	5	3	34	42	0	0	36	36
- Maßnahmen gegen Hardwarediebstahl	107	28	9	144	50	18	28	96	51	24	26	101
physikalisches Löschen von Datenträgern	123	22	17	162	69	18	21	108	51	14	26	91
Unterbrechungsfreie Stromversorgung	232	4	4	240	47	5	27	79	14	0	35	49
Klimatisierung	221	6	8	235	21	0	32	53	13	0	35	48

Rückrufautomatik bei Modemzugriff	117	21	14	152	29	10	22	61	36	11	24	71
Reserve-Netzzugang zur Ausfallüberbrückung	136	26	10	172	51	7	17	75	34	4	23	61

	Server			Clients			mobile Endgeräte (Notebooks, PDAs)		
	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen
Firewalls	98%	2%	0%	58%	4%	39%	48%	5%	47%
Virenschutzmechanismen	98%	1%	2%	97%	2%	2%	88%	6%	6%
Intrusion Detection System	43%	44%	13%	12%	31%	57%	5%	30%	65%
Benutzerverzeichnis mit Security-Policy	69%	22%	9%	61%	18%	20%	59%	16%	25%
Authentisierung	98%	26%	16%	97%	31%	15%	95%	27%	16%
- Hardware Token	37%	25%	38%	39%	24%	37%	49%	17%	33%
- Passwort	98%	0%	2%	96%	0%	3%	94%	2%	4%
- Chipkarte	9%	52%	39%	20%	51%	29%	20%	45%	35%
- biometrische Verfahren	5%	37%	58%	3%	40%	56%	0%	29%	71%
Protokollierung unberechtigter Zugriffe	87%	11%	1%	72%	7%	21%	71%	4%	25%
Content Inspection/Filtering (Adress-/Inhaltsfilter)	66%	20%	14%	32%	28%	41%	31%	19%	50%
Proxy-Server	91%	6%	4%	67%	7%	26%	57%	10%	33%
Public Key Infrastructure (PKI)	20%	63%	17%	23%	55%	23%	18%	51%	31%
Verschlüsselung	70%	56%	17%	67%	51%	18%	67%	60%	18%
- sensitive Dateien	49%	38%	13%	53%	33%	13%	58%	31%	11%
- Festplatten (kpl.)	25%	47%	27%	24%	44%	31%	41%	47%	12%
- Archivdatenträger/Backups	44%	26%	30%	25%	33%	42%	26%	29%	45%
- LAN / Intranet-	49%	33%	18%	50%	26%	24%	41%	34%	25%

Verbindungen									
- WAN / Internet-Verbindungen	57%	33%	10%	61%	22%	17%	54%	23%	23%
- Telefon	25%	19%	56%	20%	12%	67%	10%	18%	71%
- Fax	19%	13%	67%	23%	4%	73%	16%	10%	73%
- E-Mail	44%	43%	13%	51%	37%	12%	43%	42%	15%
Physische Sicherheit	99%	30%	13%	85%	26%	21%	66%	29%	26%
- Zutrittskontrolle	92%	5%	3%	75%	8%	17%	54%	9%	37%
- Bewachung	79%	8%	13%	59%	6%	35%	35%	4%	61%
- Video-Überwachung	61%	15%	24%	25%	15%	60%	2%	12%	85%
- Einbruchsmeldesysteme	90%	5%	5%	69%	4%	27%	41%	5%	53%
- Schutz von Glasflächen gegen Durchbruch / Durchwurf	83%	6%	11%	54%	0%	46%	16%	0%	84%
- Sicherheitstüren	88%	8%	4%	57%	9%	35%	33%	6%	61%
- Brandmeldesysteme	93%	4%	3%	80%	1%	19%	47%	0%	53%
- Löschanlagen	77%	13%	10%	45%	8%	46%	15%	7%	78%
- andere Meldesystem (z. B. Gas, Staub, Wasser)	73%	7%	20%	26%	0%	74%	10%	7%	83%
- Datensicherungsschränke/-räume	93%	4%	4%	58%	6%	35%	43%	0%	57%
- Schutz gegen kompromittierend Abstrahlung	46%	10%	44%	12%	7%	81%	0%	0%	100%
- Maßnahmen gegen Hardwarediebstahl	74%	19%	6%	52%	19%	29%	50%	24%	26%
physikalisches Löschen von Datenträgern	76%	14%	10%	64%	17%	19%	56%	15%	29%
Unterbrechungsfreie Stromversorgung	97%	2%	2%	59%	6%	34%	29%	0%	71%

Klimatisierung	94%	3%	3%	40%	0%	60%	27%	0%	73%
Rückrufautomatik bei Modemzugriff	77%	14%	9%	48%	16%	36%	51%	15%	34%
Reserve-Netzzugang zur Ausfallüberbrückung	79%	15%	6%	68%	9%	23%	56%	7%	38%

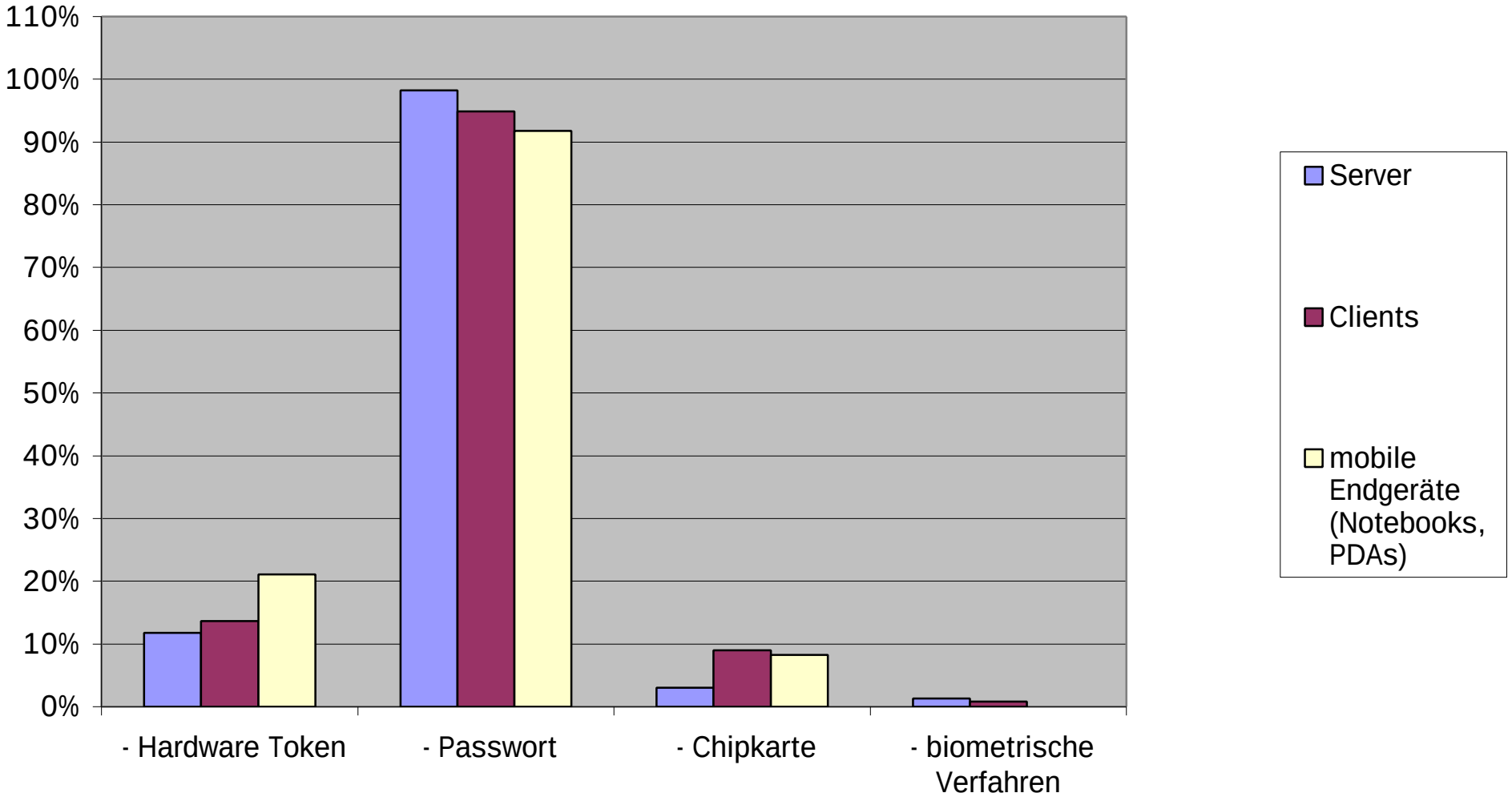
Gesamtansicht der Maßnahmen die realisiert wurden

	Server	Clients	mobile Endgeräte (Notebooks, PDAs)
	realisiert	realisiert	realisiert
Firewalls	98%	58%	48%
Virenschutzmechanismen	98%	97%	88%
Intrusion Detection System	43%	12%	5%
Benutzerverzeichnis mit Security-Policy	69%	61%	59%
Authentisierung	98%	97%	95%
Protokollierung unberechtigter Zugriffe	87%	72%	71%
Content Inspection/Filtering (Adress-/Inhaltsfilter)	66%	32%	31%
Proxy-Server	91%	67%	57%
Public Key Infrastructure (PKI)	20%	23%	18%
Verschlüsselung	70%	67%	67%
Physische Sicherheit	99%	85%	66%
physikalisches Löschen von Datenträgern	76%	64%	56%
Unterbrechungsfreie Stromversorgung	97%	59%	29%
Klimatisierung	94%	40%	27%
Rückrufautomatik bei Modemzugriff	77%	48%	51%
Reserve-Netzzugang zur Ausfallüberbrückung	79%	68%	56%

Detaillierte Übersicht der Maßnahmen zur Authentisierung

	Server	Clients	mobile Endgeräte (Notebooks, PDAs)
	realisiert	realisiert	realisiert
Authentisierung	100%=229	100%=234	100%=218
- Hardware Token	12%	14%	21%
- Passwort	98%	95%	92%
- Chipkarte	3%	9%	8%
- biometrische Verfahren	1%	1%	0%

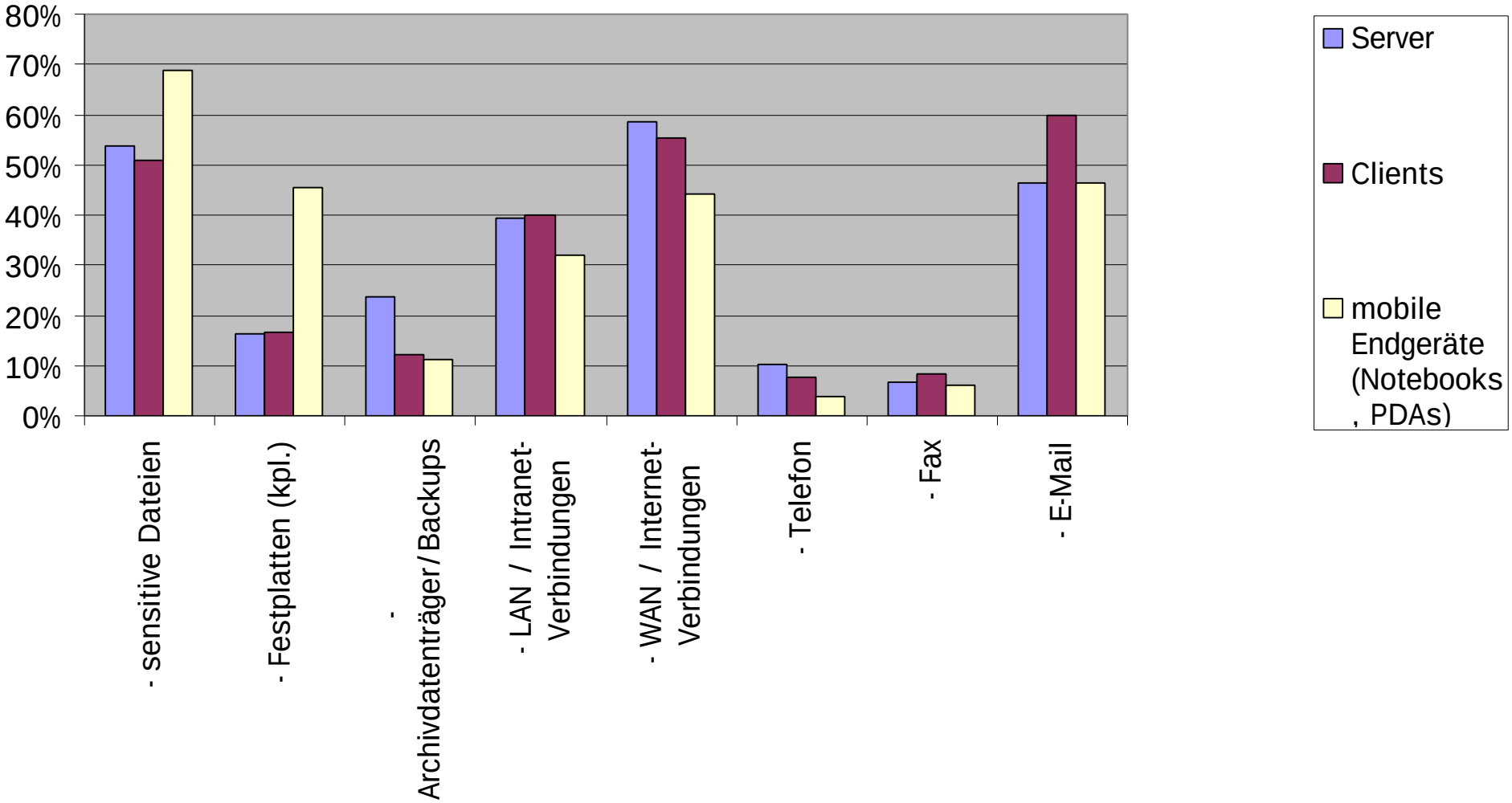
Maßnahmen zur Authentisierung



Detaillierte Übersicht der Maßnahmen zur Verschlüsselung

	Server	Clients	mobile Endgeräte (Notebooks, PDAs)
	realisiert	realisiert	realisiert
Verschlüsselung	100%=147	100%=132	100%=134
- sensitive Dateien	54%	51%	69%
- Festplatten (kpl.)	16%	17%	46%
- Archivdatenträger/Backups	24%	12%	11%
- LAN / Intranet-Verbindungen	39%	40%	32%
- WAN / Internet-Verbindungen	59%	55%	44%
- Telefon	10%	8%	4%
- Fax	7%	8%	6%
- E-Mail	46%	60%	46%

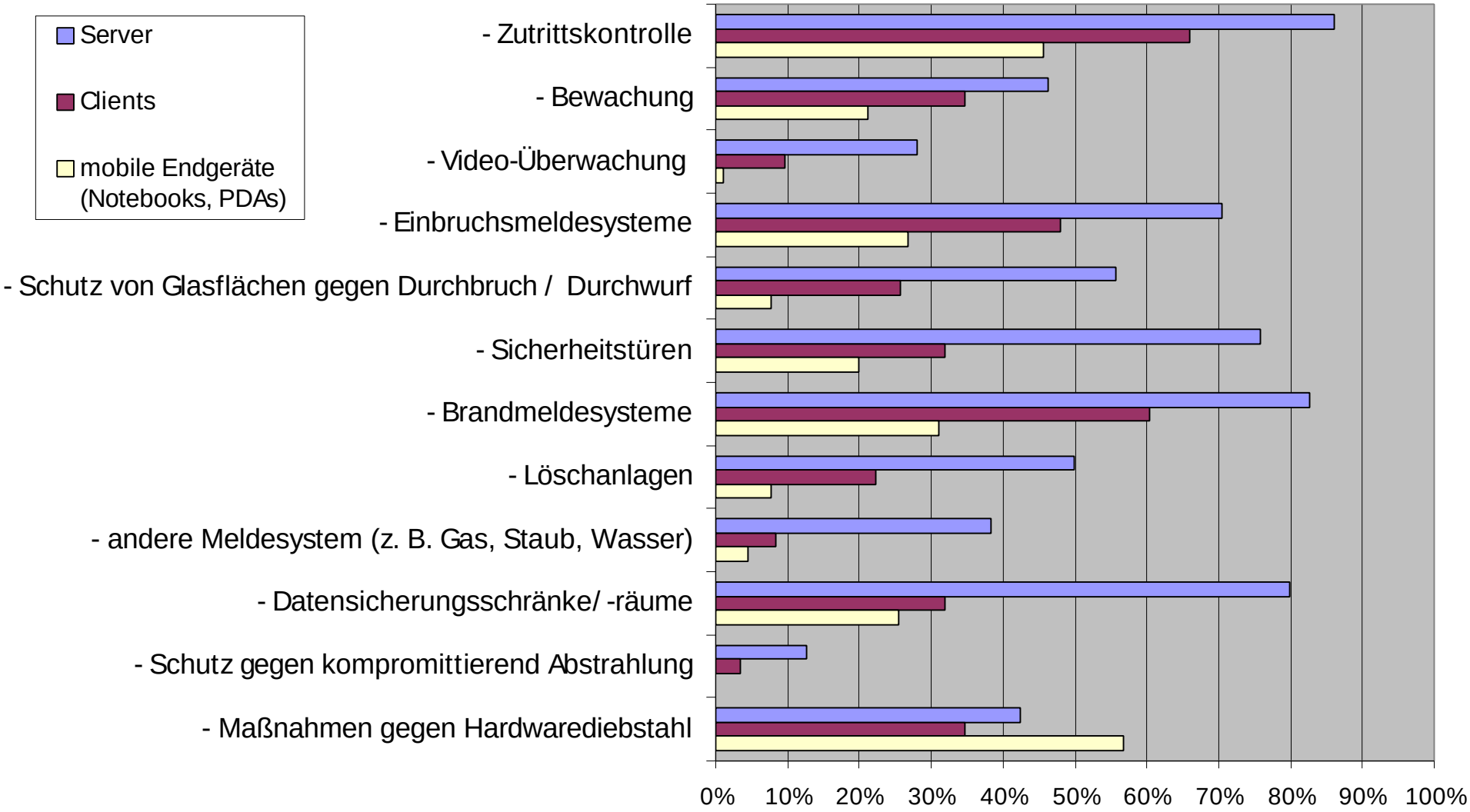
Maßnahmen zur Verschlüsselung



Detaillierte Übersicht der Maßnahmen zur Physische Sicherheit

	Server	Clients	mobile Endgeräte (Notebooks, PDAs)
	realisiert	realisiert	realisiert
Physische Sicherheit	100%=253	100%=144	100%=90
- Zutrittskontrolle	86%	66%	46%
- Bewachung	46%	35%	21%
- Video-Überwachung	28%	10%	1%
- Einbruchsmeldesysteme	70%	48%	27%
- Schutz von Glasflächen gegen Durchbruch / Durchwurf	56%	26%	8%
- Sicherheitstüren	76%	32%	20%
- Brandmeldesysteme	83%	60%	31%
- Löschanlagen	50%	22%	8%
- andere Meldesystem (z. B. Gas, Staub, Wasser)	38%	8%	4%
- Datensicherungsschränke/-räume	80%	32%	26%
- Schutz gegen kompromittierend Abstrahlung	13%	3%	0%
- Maßnahmen gegen Hardwarediebstahl	42%	35%	57%

Maßnahmen zur Physischen Sicherheit

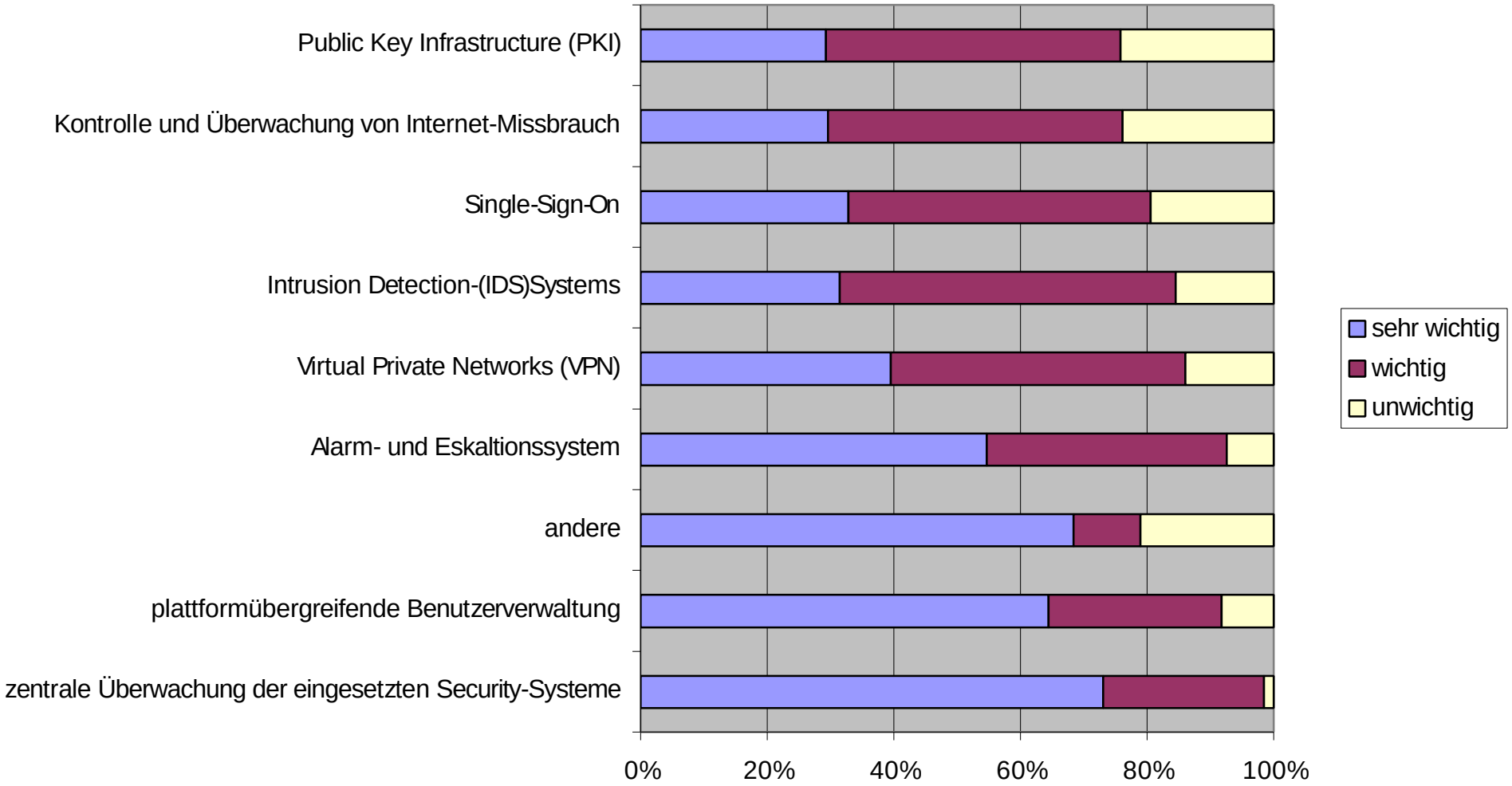


5.02

Wie wichtig bewerten Sie folgende Komponenten eines unternehmensweiten Security-Managements?								
	sehr wichtig (2)	wichtig (1)	unwichtig (0)	Summe	sehr wichtig	wichtig	unwichtig	Bedeutungskennzahl
zentrale Überwachung der eingesetzten Security-Systeme	190	66	4	260	73%	25%	2%	1,72
plattformübergreifende Benutzerverwaltung	165	70	21	256	64%	27%	8%	1,56
andere	13	2	4	19	68%	11%	21%	1,47
Alarm- und Eskaltionssystem	140	97	19	256	55%	38%	7%	1,47
Virtual Private Networks (VPN)	102	120	36	258	40%	47%	14%	1,26
Intrusion Detection-(IDS)Systems	77	130	38	245	31%	53%	16%	1,16
Single-Sign-On	81	118	48	247	33%	48%	19%	1,13
Kontrolle und Überwachung von Internet-Missbrauch	77	121	62	260	30%	47%	24%	1,06
Public Key Infrastructure (PKI)	75	119	62	256	29%	46%	24%	1,05

Andere Nennungen
Mitarbeiter-Qualifikation, Mitarbeiter Schulung / Betriebsklima, durchgängige Verschlüsselungssoftware auf allen Plattformen bis E-Mail

Komponenten des Security-Managements

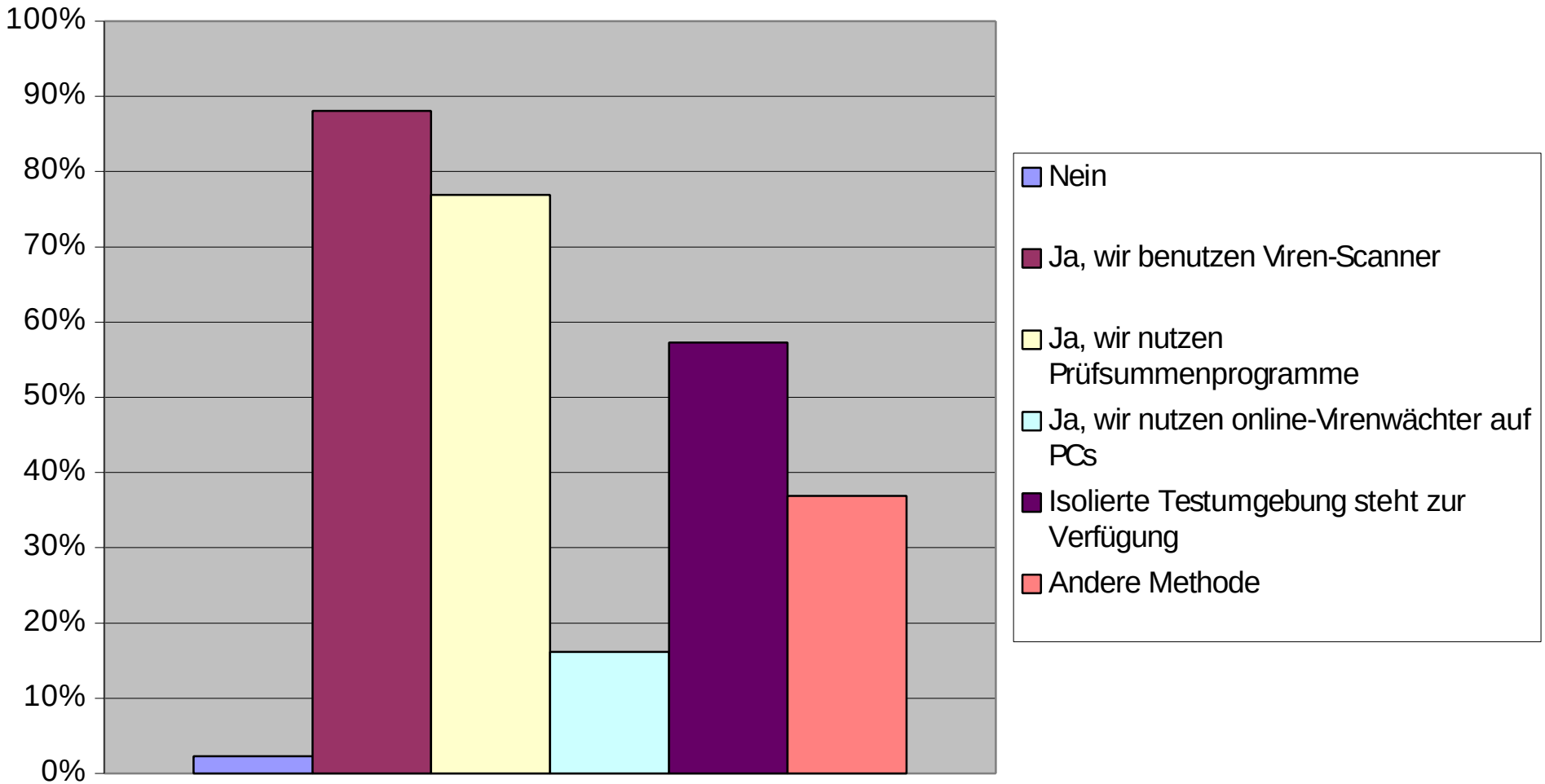


5.03

Haben Sie Vorsorge gegen Malware getroffen? (Mehrfachnennungen möglich)		
Basis der Prozentuierung:	260	
	Nennungen	Prozentual
Nein	6	2%
Ja, wir benutzen Viren-Scanner	229	88%
an der Firewall/Internet-Gateway	229	88%
auf dem Mail-/File-/Applikationsserver	200	77%
auf den PCs/Workstations	186	72%
Ja, wir nutzen Prüfsummenprogramme	200	77%
Ja, wir nutzen online-Virenwächter auf PCs	42	16%
Isolierte Testumgebung steht zur Verfügung	149	57%
Andere Methode	96	37%

Andere Methoden
Filter gegen ausführbare Dateien, Schulungen, Information der Mitarbeiter, Ausschluß bestimmter Dienste (z. B. HTTPS), Eigenentwicklung

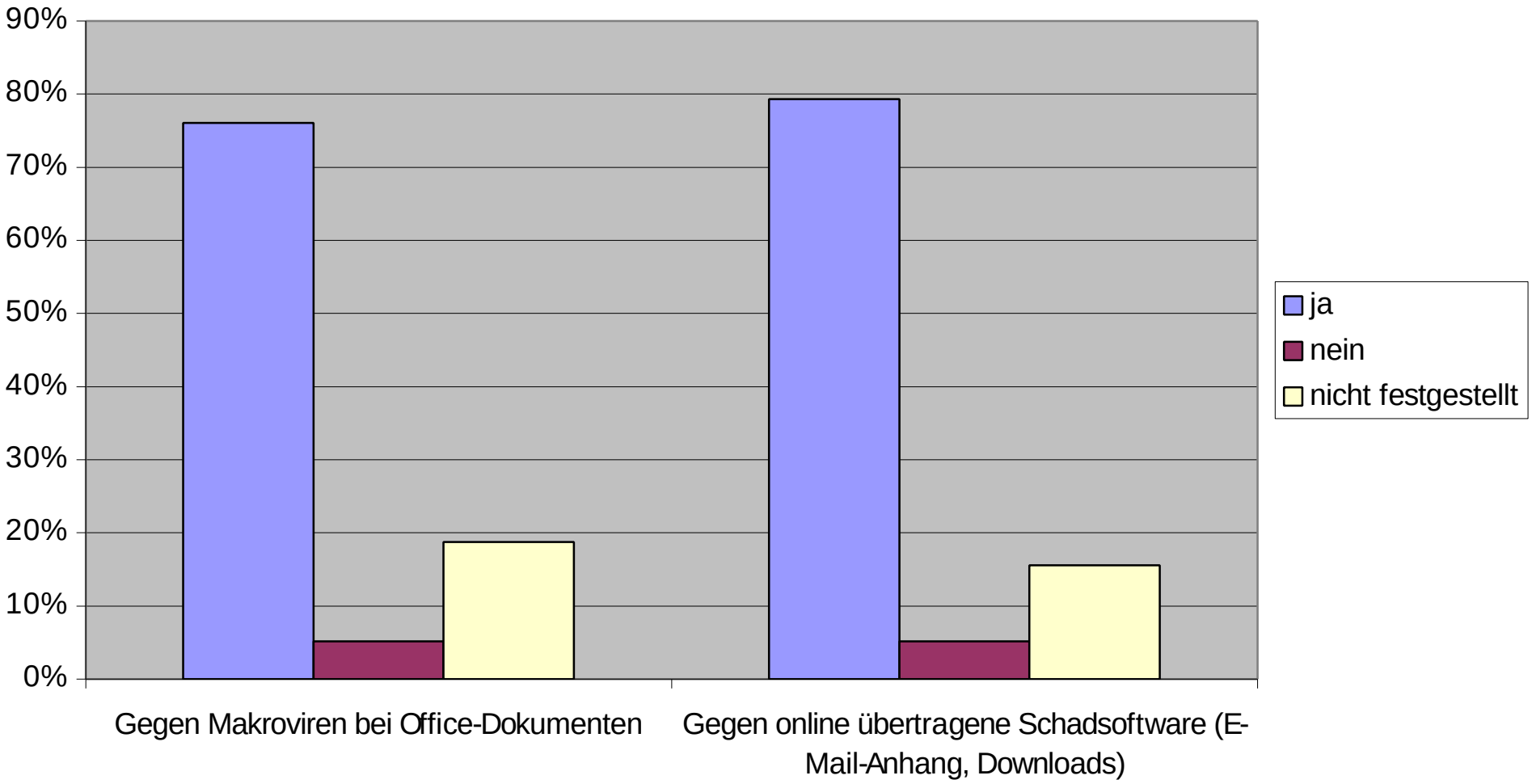
Vorsorge gegen Malware



5.03a

Ist sichergestellt, dass Ihre Maßnahmen auch wirken ?							
	ja	nein	nicht festgestellt	Summe	ja	nein	nicht festgestellt
Gegen Makroviren bei Office-Dokumenten	191	13	47	251	76%	5%	19%
Gegen online übertragene Schadsoftware (E-Mail-Anhang, Downloads)	199	13	39	251	79%	5%	16%

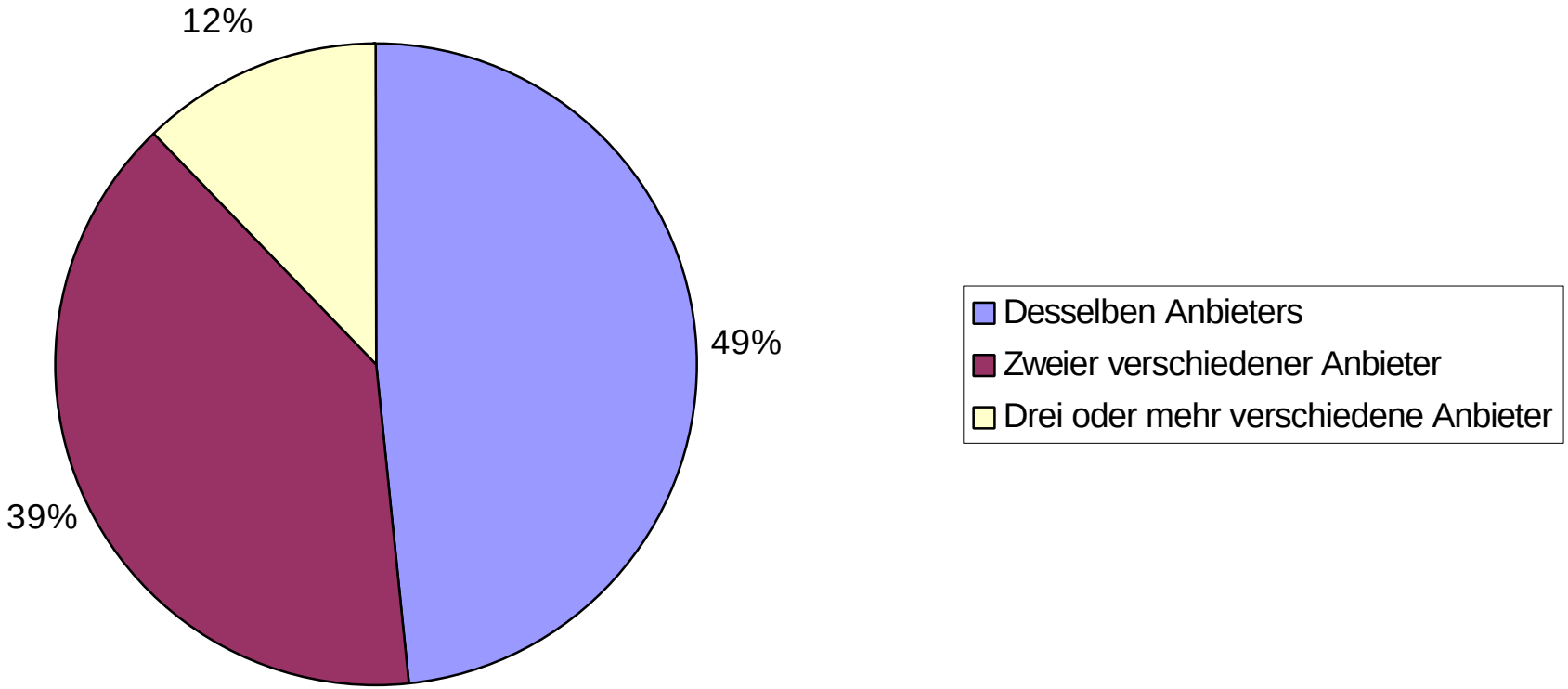
Wirksamkeit der Maßnahmen



5.03b

Nutzen Sie auf Server/Gateway und PCs aus Sicherheitsgründen Anti-Viren-Software:		
	Anzahl	Prozent
Desselben Anbieters	119	48%
Zweier verschiedener Anbieter	97	39%
Drei oder mehr verschiedene Anbieter	30	12%
Summe	246	

Server/ Gateway & PC´ s - Anti-Viren-Software

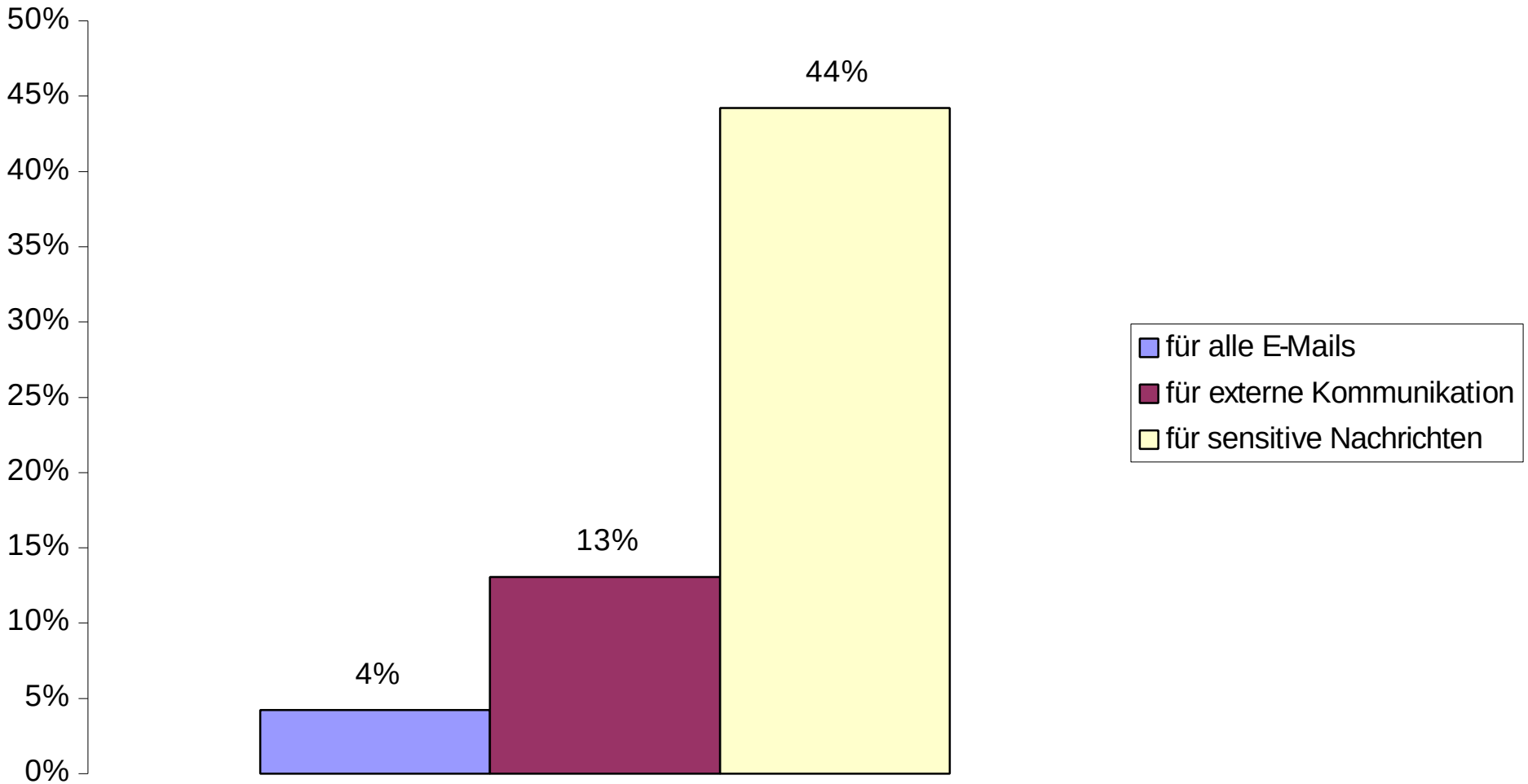


5.04

Nutzen Sie in Ihrem Unternehmen E-Mail-Verschlüsselung - sofern der Kommunikationspartner über einen Kryptoschlüssel verfügt? (Mehrfachnennungen möglich)		
Basis der Prozentuierung: 260		
	Nennungen	Prozentual
für alle E-Mails	11	4%
für externe Kommunikation	34	13%
für sensitive Nachrichten	115	44%

Keine Angaben: 120

Nutzung der E-Mailverschlüsselung

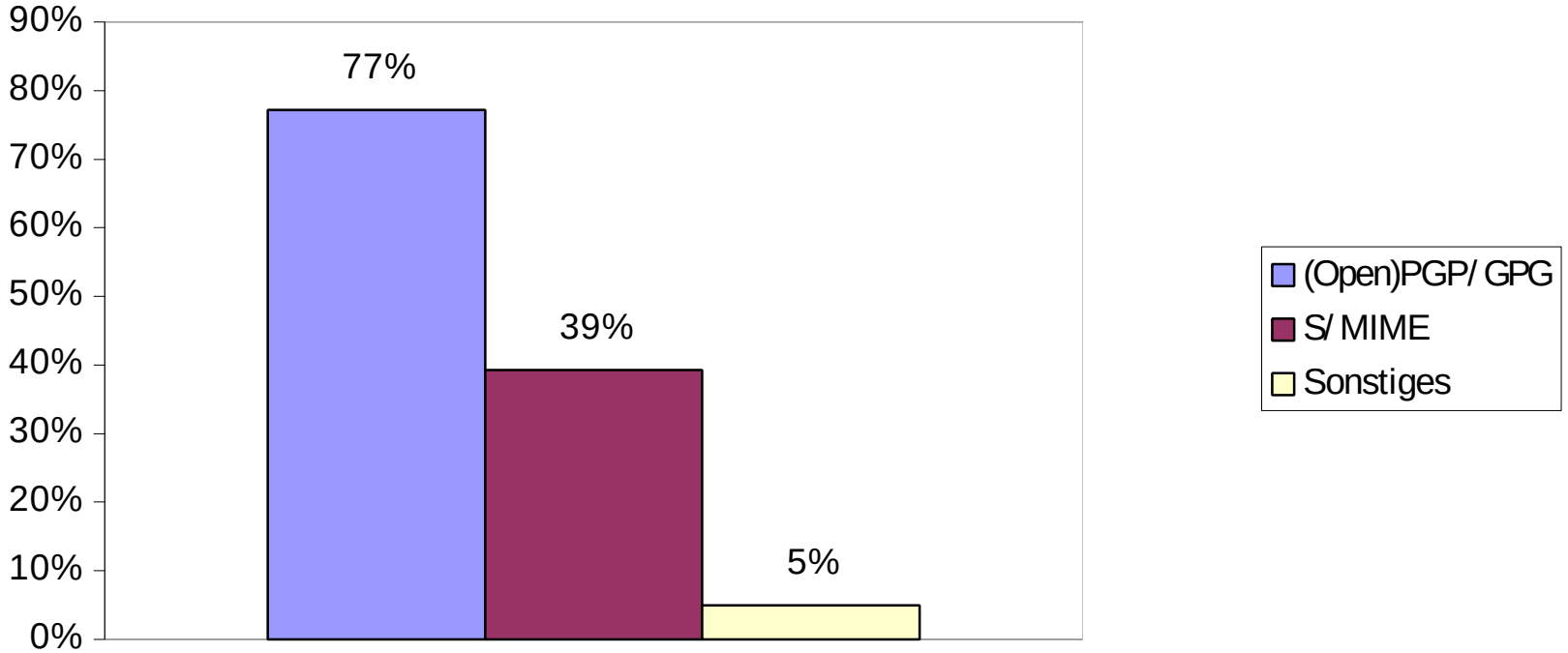


5.04a

Welchen Standard verwende Sie dabei? (Mehrfachnennungen möglich)		
Basis der Prozentuierung:	140	
	Nennungen	Prozentual
S/MIME	55	39%
(Open)PGP/GPG	108	77%
Sonstiges	7	5%

Liste Sonstige
Lotus-Notes, interne Notes-Funktoinalitäten, BSI-Kryptogeräte, Eigenentwicklung

Eingesetzter Standard



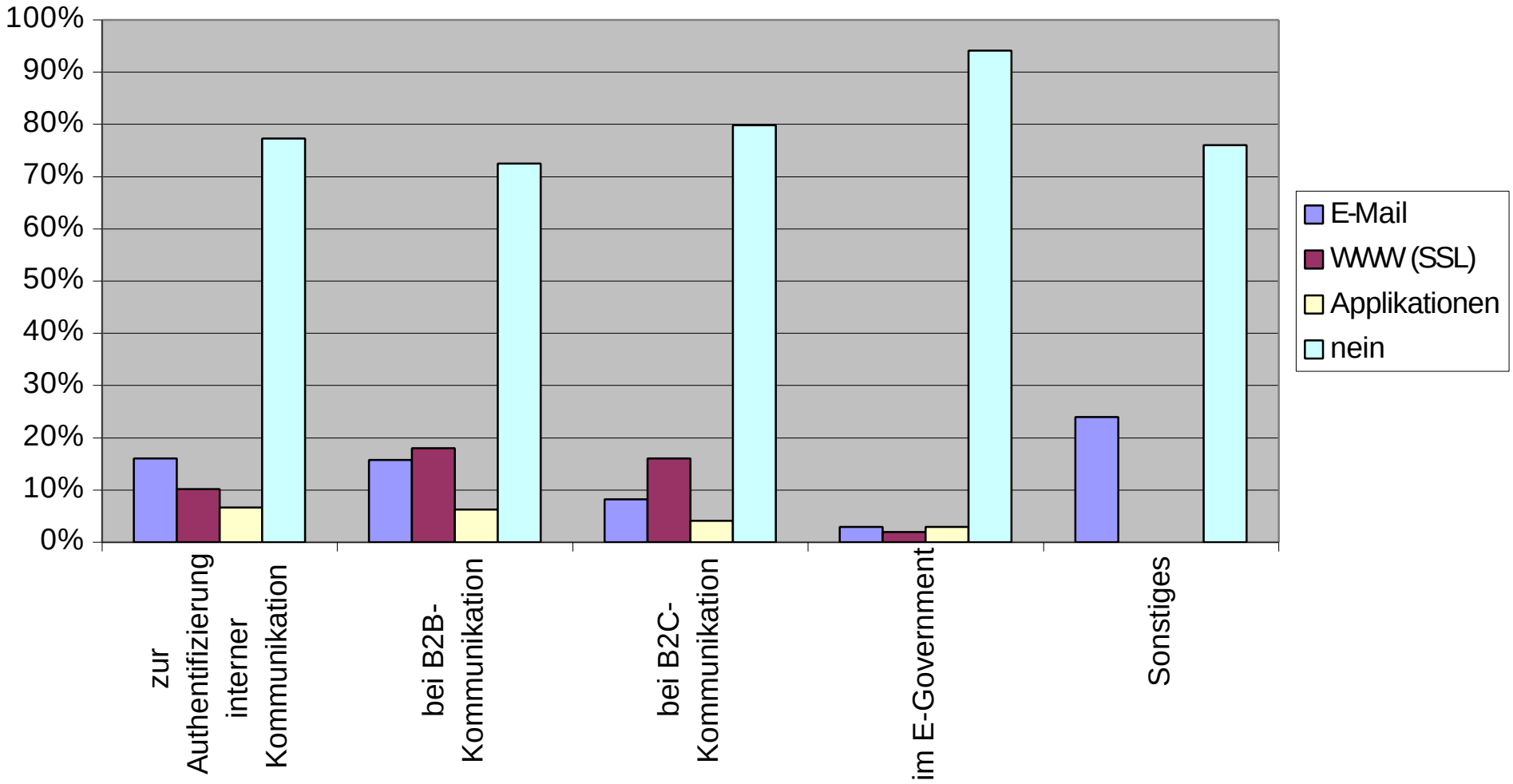
5.05

Nutzen Sie in Ihrem Unternehmen digitale/elektronische Signaturen? (Mehrfachnennungen möglich)					
Basis (260 - keine Angaben)					
	E-Mail	WWW (SSL)	Applikationen	nein	Keine Angaben
zur Authentifizierung interner Kommunikation	36	23	15	174	35
bei B2B-Kommunikation	35	40	14	161	38
bei B2C-Kommunikation	18	35	9	174	42
im E-Government	6	4	6	191	57
Sonstiges	6	0	0	19	235

Keine Angaben: 22

	E-Mail	WWW (SSL)	Applikationen	nein
zur Authentifizierung interner Kommunikation	16%	10%	7%	77%
bei B2B-Kommunikation	16%	18%	6%	73%
bei B2C-Kommunikation	8%	16%	4%	80%
im E-Government	3%	2%	3%	94%
Sonstiges	24%	0%	0%	76%

Digitale/ elektronische Signaturen



5.05a

Welche Infrastruktur nutzten Sie für digitale/elektronische Signaturen?																
	B2B-Server				B2C-Server				Client/PC				mobile Endgeräte			
	realisiert	geplant	nicht vorgesehen	Summe	realisiert	geplant	nicht vorgesehen	Summe	realisiert	geplant	nicht vorgesehen	Summe	realisiert	geplant	nicht vorgesehen	Summe
nur Software	39	5	23	67	30	7	20	57	48	11	16	75	43	2	22	67
Hardwaremodule	4	7	37	48	4	7	34	45	0	5	44	49	4	7	35	46
Hardware-Token	7	7	34	48	4	7	36	47	12	4	33	49	4	8	34	46
Chipkareten	14	6	36	56	11	6	33	50	21	11	25	57	4	15	28	47
"Klasse-2"-Chipkartenterminal (sichere PIN-Eingabe)	6	4	39	49	4	2	41	47	6	2	40	48	0	2	43	45
"Klasse-3"-Chipkartenterminal (mit eigenem Display)	5	0	40	45	3	1	41	45	3	0	43	46	0	0	43	43
lt. SigG	0	5	32	37	3	4	31	38	3	4	33	40	0	2	35	37
- fortgeschrittene Signatur	7	11	28	46	4	11	27	42	3	11	33	47	0	6	35	41
- qualifizierte Signatur	3	6	35	44	0	9	31	40	7	11	37	55	2	10	35	47
- qualifizierte Signatur mit Anbieterakkreditierung	7	2	37	46	6	5	31	42	5	5	41	51	2	2	41	45
Sonstiges	0	0	0	0	0	0	2	2	0	0	2	2	4	0	3	7
nichts von alledem	0	0	6	6	41	6	0	47	42	6	0	48	48	11	0	59

Keine Angaben: 96

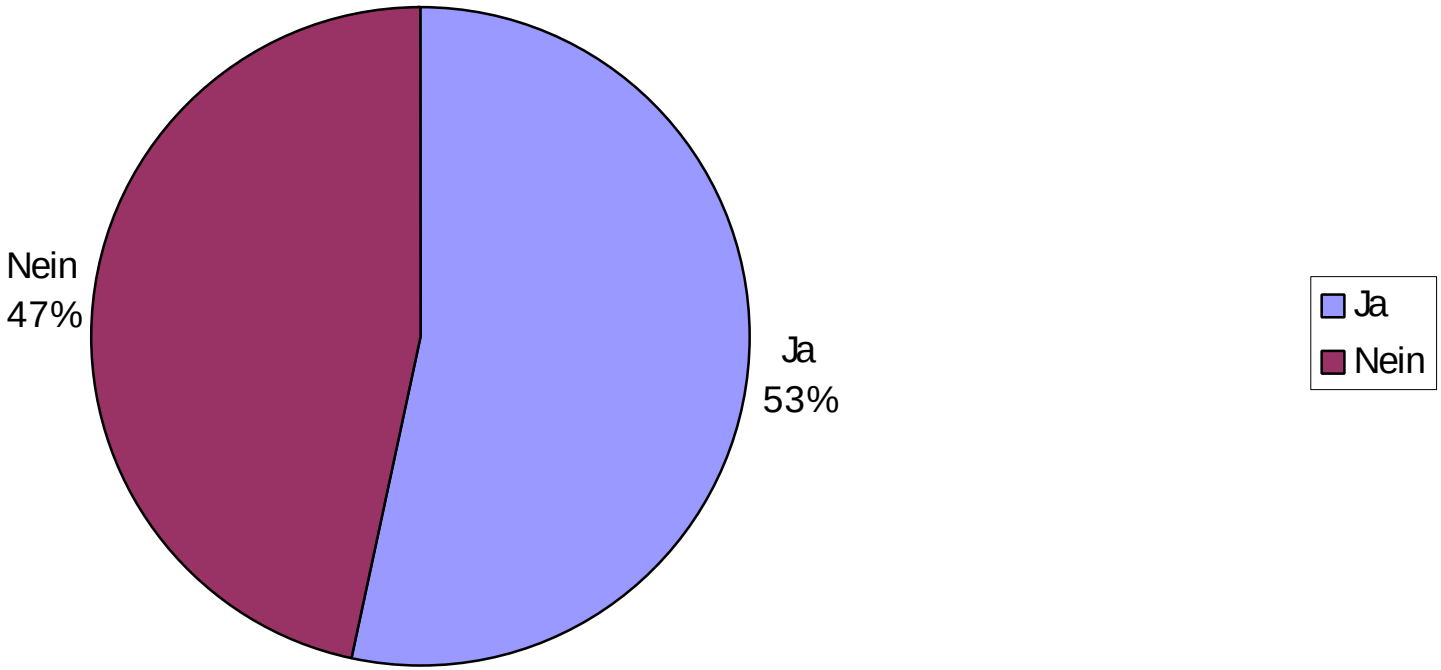
	B2B-Server			B2C-Server			Client/PC			mobile Endgeräte		
	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen
nur Software	58%	7%	34%	53%	12%	35%	64%	15%	21%	64%	3%	33%
Hardwaremodule	8%	15%	77%	9%	16%	76%	0%	10%	90%	9%	15%	76%
Hardware-Token	15%	15%	71%	9%	15%	77%	24%	8%	67%	9%	17%	74%
Chipkareten	25%	11%	64%	22%	12%	66%	37%	19%	44%	9%	32%	60%
"Klasse-2"-Chipkartenterminal (sichere PIN-Eingabe)	12%	8%	80%	9%	4%	87%	13%	4%	83%	0%	4%	96%
"Klasse-3"-Chipkartenterminal (mit eigenem Display)	11%	0%	89%	7%	2%	91%	7%	0%	93%	0%	0%	100%
lt. SigG	0%	14%	86%	8%	11%	82%	8%	10%	83%	0%	5%	95%
- fortgeschrittene Signatur	15%	24%	61%	10%	26%	64%	6%	23%	70%	0%	15%	85%
- qualifizierte Signatur	7%	14%	80%	0%	23%	78%	13%	20%	67%	4%	21%	74%
- qualifizierte Signatur mit Anbieterakkreditierung	15%	4%	80%	14%	12%	74%	10%	10%	80%	4%	4%	91%
Sonstiges	0%	0%	0%	0%	0%	100%	0%	0%	100%	57%	0%	43%
nichts von alledem	0%	0%	100%	87%	13%	0%	88%	13%	0%	81%	19%	0%

5.06

Planen Sie die Implementierung einer PKI?			
	Ja	Nein	Summe
	124	108	232
	53%	47%	

Keine Angaben 28

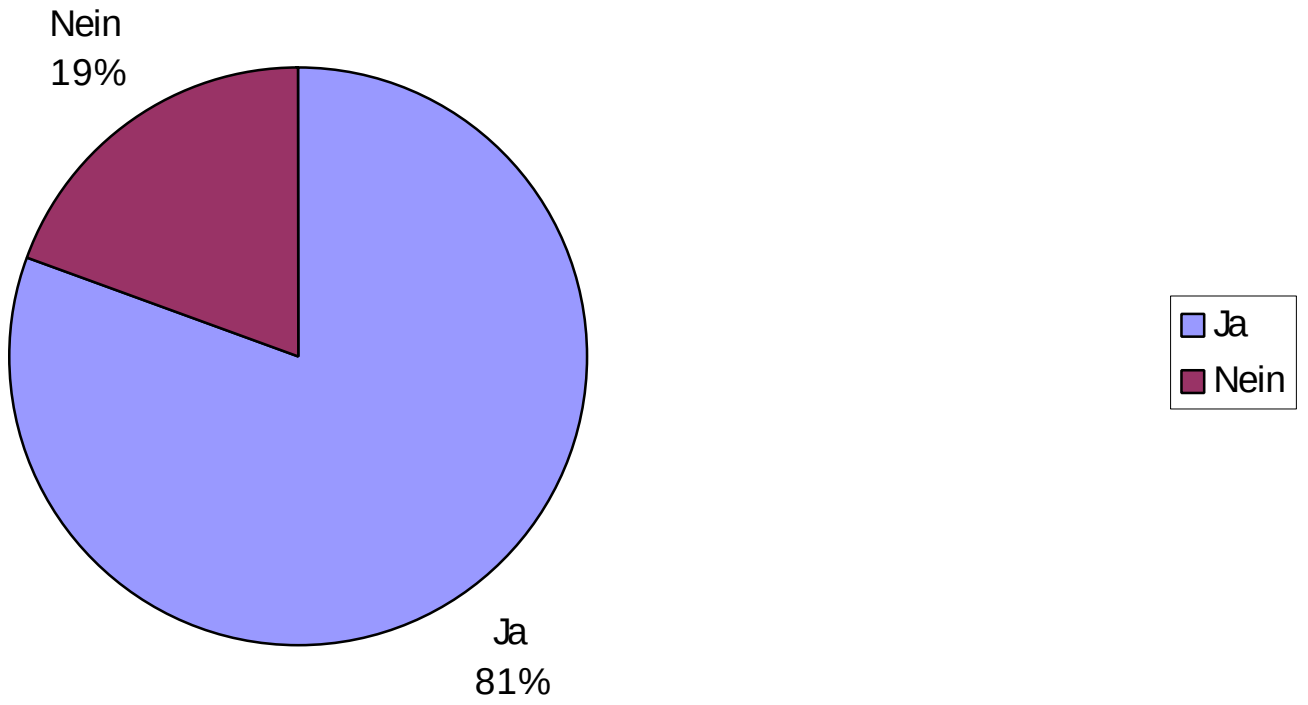
Implementierung - PKI



5.06a

Ist das Herkunftsland von PKI-Lösungen für Sie von Bedeutung?			
	Ja	Nein	Summe
	100	24	124
	81%	19%	

Bedeutung des Herkunftslandes einer PKI-Lösung

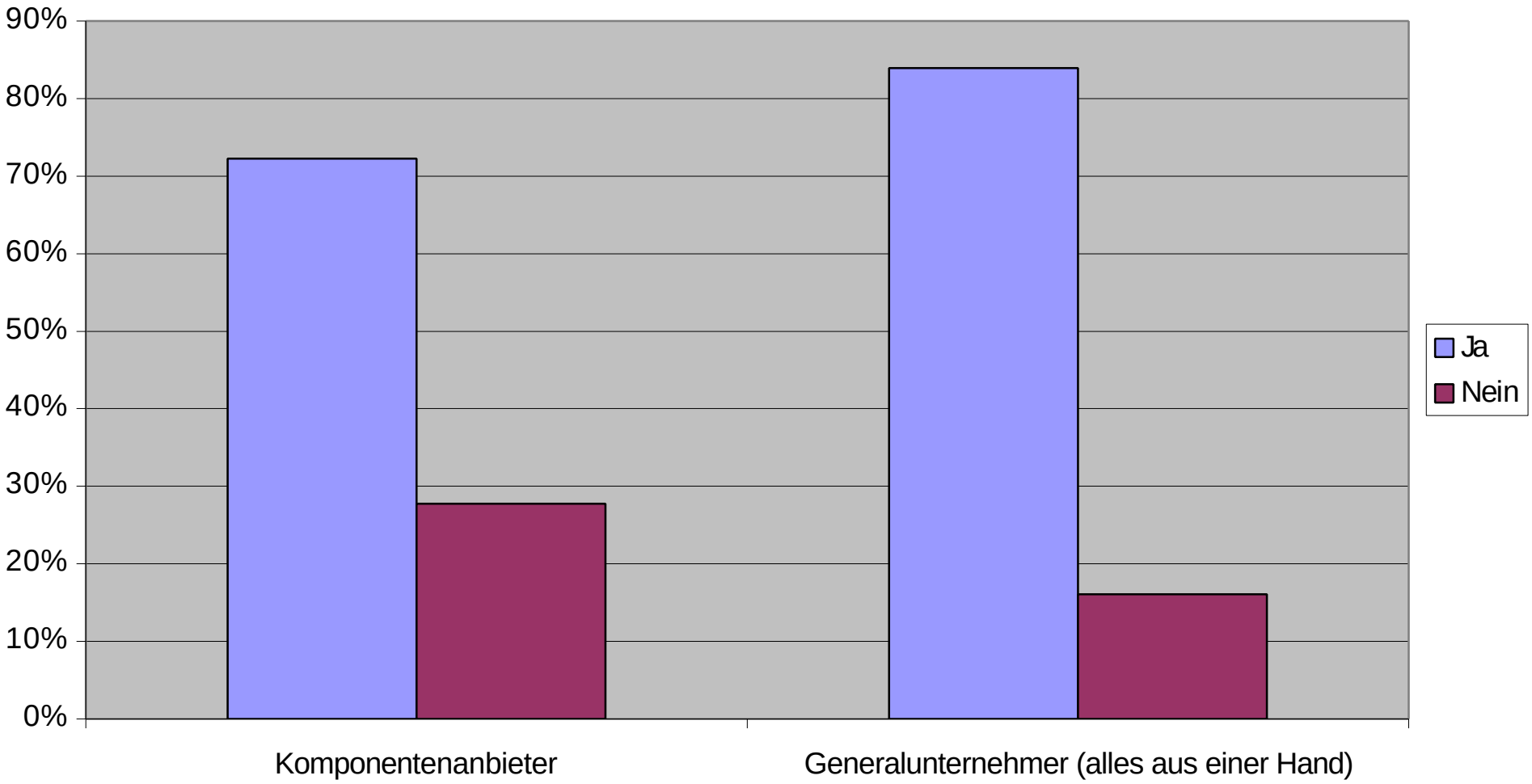


5.06b

Bevorzugen Sie PKI-Lösungsanbieter als			
	Ja	Nein	Summe
Komponentenanbieter	65	25	90
Generalunternehmer (alles aus einer Hand)	99	19	118

	Ja	Nein
Komponentenanbieter	72%	28%
Generalunternehmer (alles aus einer Hand)	84%	16%

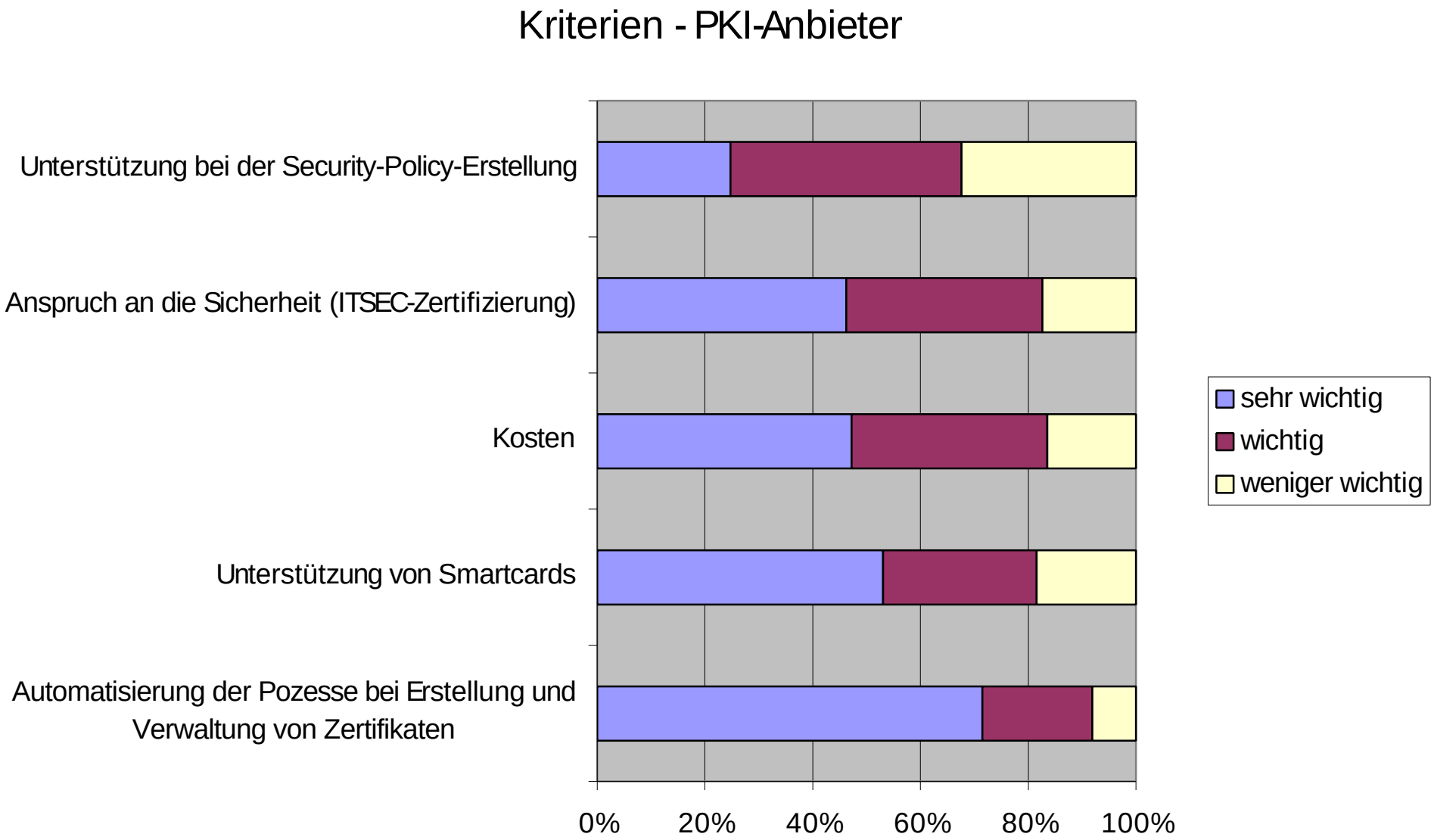
PKI-Lösungsanbieter



5.06c

Wie wichtig sind Ihnen folgende Kriterien bei der Auswahl eines PKI-Anbieters					
	sehr wichtig (2)	wichtig (1)	weniger wichtig (0)	Summe	Bedeutungsfaktor
Automatisierung der Pozesse bei Erstellung und Verwaltung von Zertifikaten	133	38	15	186	1,63
Unterstützung von Smartcards	95	51	33	179	1,35
Kosten	86	66	30	182	1,31
Anspruch an die Sicherheit (ITSEC-Zertifizierung)	85	67	32	184	1,29
Unterstützung bei der Security-Policy-Erstellung	45	78	59	182	0,92

	sehr wichtig	wichtig	weniger wichtig
Automatisierung der Pozesse bei Erstellung und Verwaltung von Zertifikaten	72%	20%	8%
Unterstützung von Smartcards	53%	28%	18%
Kosten	47%	36%	16%
Anspruch an die Sicherheit (ITSEC-Zertifizierung)	46%	36%	17%
Unterstützung bei der Security-Policy-Erstellung	25%	43%	32%

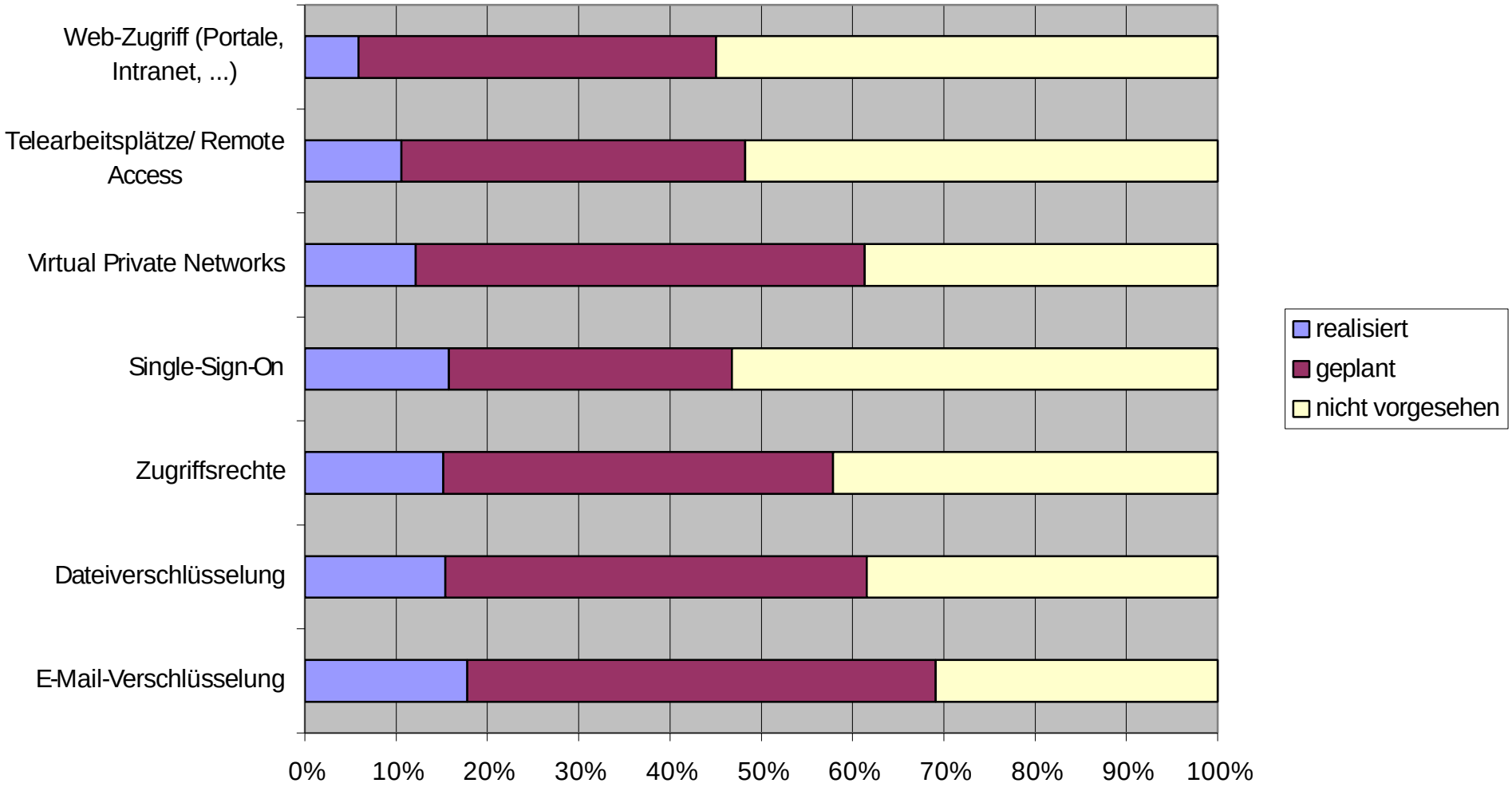

Kriterien - PKI-Anbieter
Unterstützung bei der Security-Policy-Erstellung
Anspruch an die Sicherheit (ITSEC-Zertifizierung)
Kosten
Unterstützung von Smartcards
Automatisierung der Pozesse bei Erstellung und Verwaltung von Zertifikaten
0%
20%
40%
60%
80%
100%
sehr wichtig
wichtig
weniger wichtig

5.06d

Für welche Zwecke nutzen Sie in Ihrem Unternehmen eine PKI?				
	realisiert	geplant	nicht vorgesehen	Summe
E-Mail-Verschlüsselung	34	98	59	191
Dateiverschlüsselung	28	84	70	182
Virtual Private Networks	27	76	75	178
Web-Zugriff (Portale, Intranet, ...)	27	53	91	171
Telearbeitsplätze/Remote Access	22	89	70	181
Zugriffsrechte	18	64	88	170
Single-Sign-On	10	67	94	171

	realisiert	geplant	nicht vorgesehen
E-Mail-Verschlüsselung	18%	51%	31%
Dateiverschlüsselung	15%	46%	38%
Zugriffsrechte	15%	43%	42%
Single-Sign-On	16%	31%	53%
Virtual Private Networks	12%	49%	39%
Telearbeitsplätze/Remote Access	11%	38%	52%
Web-Zugriff (Portale, Intranet, ...)	6%	39%	55%

Verwendungszweck - PKI



5.07

Welche Logdaten wertet Ihr Unternehmen aus?

Basis der Prozentuierung: 254

	Internet				Intranet/LAN			
	Auswertung min. 2x pro Woche	Auswertung seltener, aber regelmäßig	Auswertung erfolgt anlassbezogen	keine Auswertung oder Protokollierung	Auswertung min. 2x pro Woche	Auswertung seltener, aber regelmäßig	Auswertung erfolgt anlassbezogen	keine Auswertung oder Protokollierung
Firewall(s)	102	62	60	11	53	41	42	70
Intrusion Detection Systems	33	26	33	73	30	21	22	92
Netzkomponenten (Router, Switches etc.)	40	40	91	45	31	28	76	61
Betriebssysteme	119	32	119	27	28	36	90	43
Web-/E-Commerce-Applikationen	0	31	61	64	19	17	42	80
Sonstiges	3	4	2	4	3	2	2	6
Summe	297	195	366	224	164	145	274	352

Keine Angaben 6

	Internet				Intranet/LAN			
	Auswertung min. 2x pro Woche	Auswertung seltener, aber regelmäßig	Auswertung erfolgt anlassbezogen	keine Auswertung oder Protokollierung	Auswertung min. 2x pro Woche	Auswertung seltener, aber regelmäßig	Auswertung erfolgt anlassbezogen	keine Auswertung oder Protokollierung
Firewall(s)	34%	32%	16%	5%	32%	28%	15%	20%
Intrusion Detection Systems	11%	13%	9%	33%	18%	14%	8%	26%
Netzkomponenten (Router, Switches etc.)	13%	21%	25%	20%	19%	19%	28%	17%
Betriebssysteme	40%	16%	33%	12%	17%	25%	33%	12%
Web-/E-Commerce-Applikationen	0%	16%	17%	29%	12%	12%	15%	23%
Sonstiges	1%	2%	1%	2%	2%	1%	1%	2%

5.07a Setzen Sie Intrusion Detection Systeme ein?

Ja	Nein	Summe
82	148	230
36%	64%	

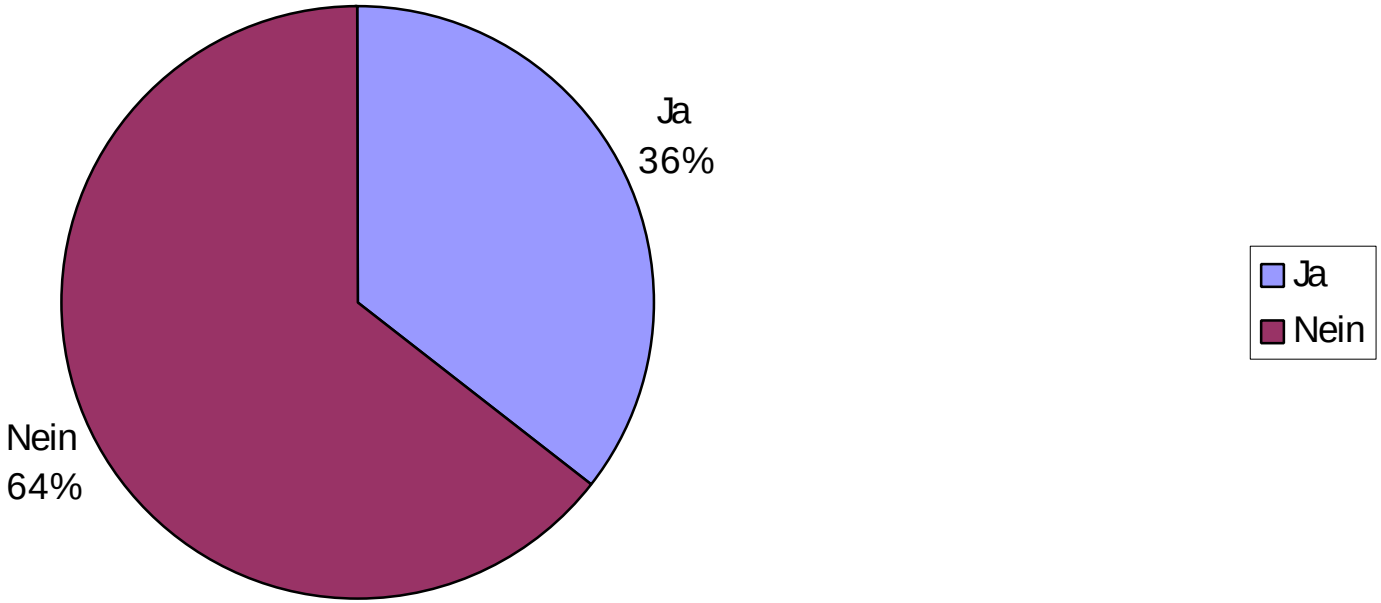
Keine Angaben: 30

	netzbasiert	hostbasiert	zentrale Auswertung der Logfiles	unveränderliche Speicherung der Logfiles
Firewall zum Internet	45	27	44	19
DMZ	35	19	28	9
Interne Firewalls	9	4	12	2
Intranet/LAN	19	10	9	6

Basis der Prozentuierung: 82

	netzbasiert	hostbasiert	zentrale Auswertung der Logfiles	unveränderliche Speicherung der Logfiles
Firewall zum Internet	55%	33%	54%	23%
DMZ	43%	23%	34%	11%
Interne Firewalls	11%	5%	15%	2%
Intranet/LAN	23%	12%	11%	7%

Intrusion Detection Systeme



5.07b

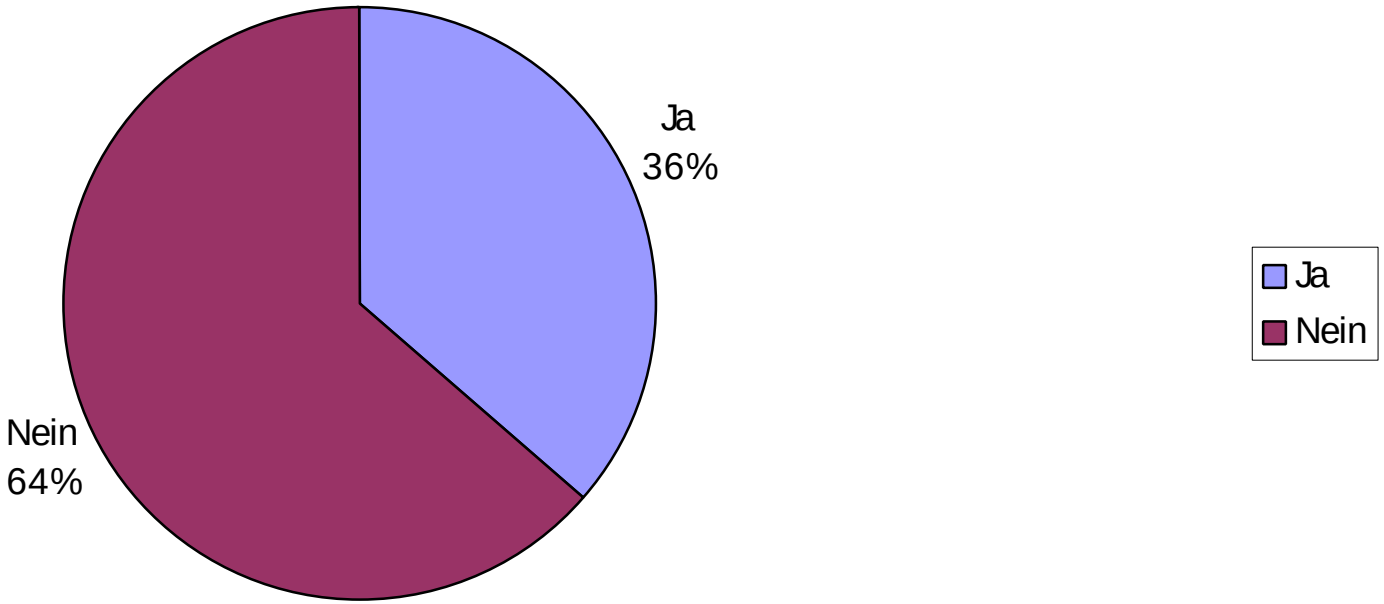
Hat Ihr Unternehmen in den letzten 12 Monaten einen Penetrationstest in Auftrag gegeben?			
	Ja	Nein	Summe
	86	151	237
	36%	64%	

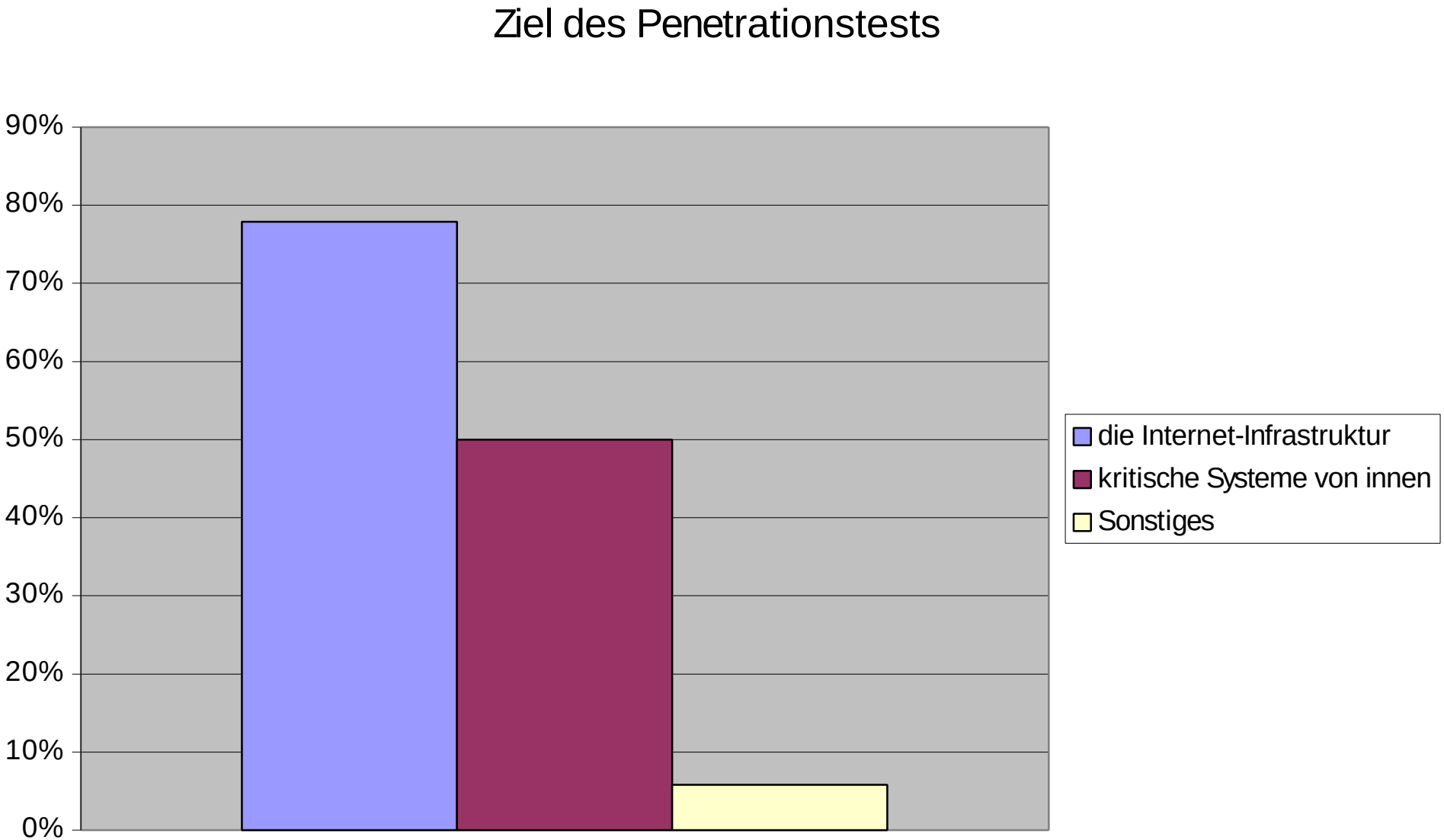
Keine Angaben: 23

(Mehrfachnennungen möglich)		
	Nennungen	Prozentual
die Internet-Infrastruktur	67	78%
kritische Systeme von innen	43	50%
Sonstiges	5	6%

Basis der Prozentuierung: 86

Penetrationstest in den letzten 12 Monaten



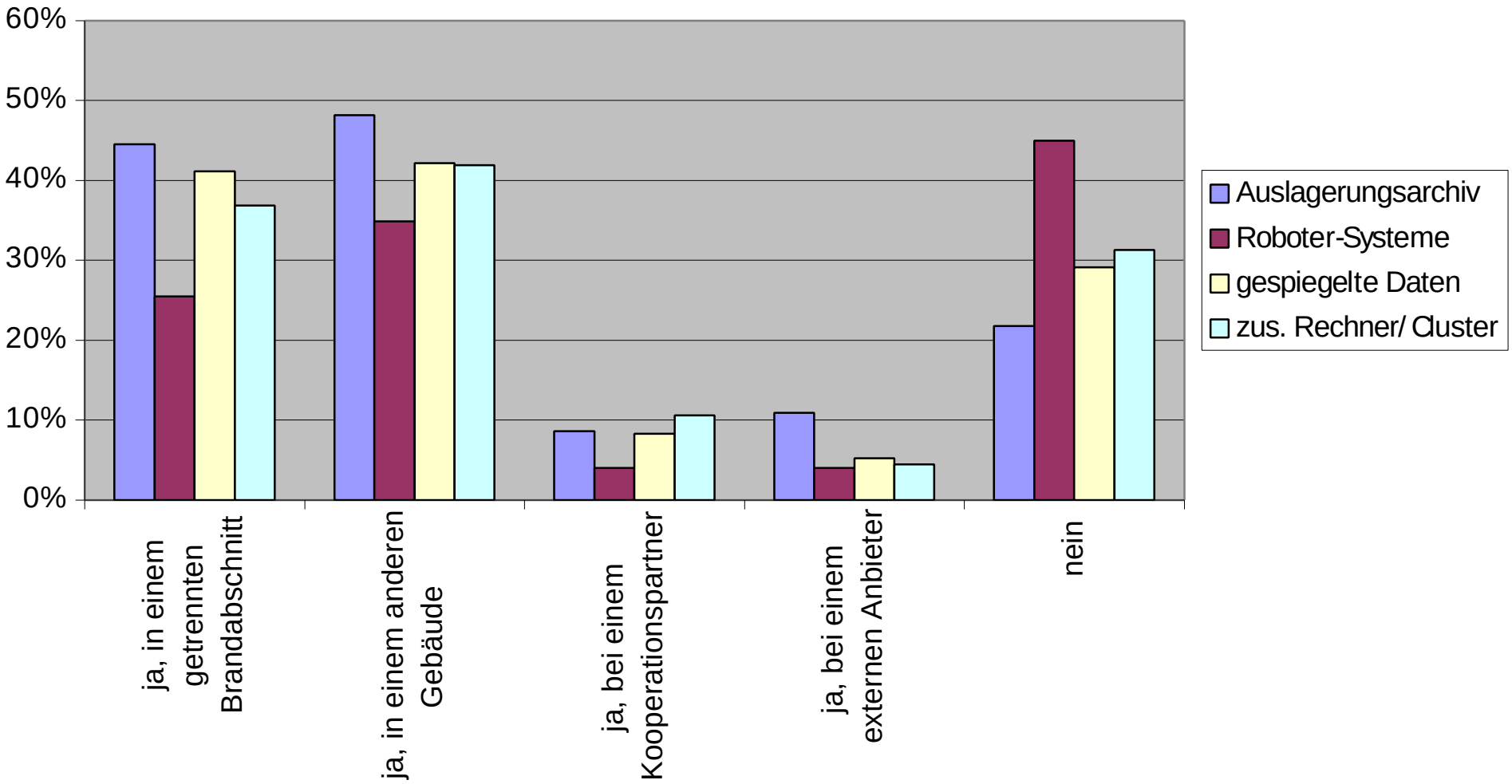

Ziel des Penetrationstests
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
die Internet-Infrastruktur
kritische Systeme von innen
Sonstiges

5.08

Halten Sie wesentliche Komponenten Ihrer Informationsverarbeitung an verschiedenen Orten vor? (Mehrfachnennungen möglich)				
Basis der Prozentuierung:	260 - k. A. aus den Spalten			
	Auslagerungsarchiv	Roboter-Systeme	gespiegelte Daten	zus. Rechner/ Cluster
ja, in einem getrennten Brandabschnitt	98	38	79	66
ja, in einem anderen Gebäude	106	52	81	75
ja, bei einem Kooperationspartner	19	6	16	19
ja, bei einem externen Anbieter	24	6	10	8
nein	48	67	56	56
Keine Angaben:	40	111	68	81

	Auslagerungsarchiv	Roboter-Systeme	gespiegelte Daten	zus. Rechner/ Cluster
ja, in einem getrennten Brandabschnitt	45%	26%	41%	37%
ja, in einem anderen Gebäude	48%	35%	42%	42%
ja, bei einem Kooperationspartner	9%	4%	8%	11%
ja, bei einem externen Anbieter	11%	4%	5%	4%
nein	22%	45%	29%	31%

Vorhaltung - wesentlicher Komponenten



5.09

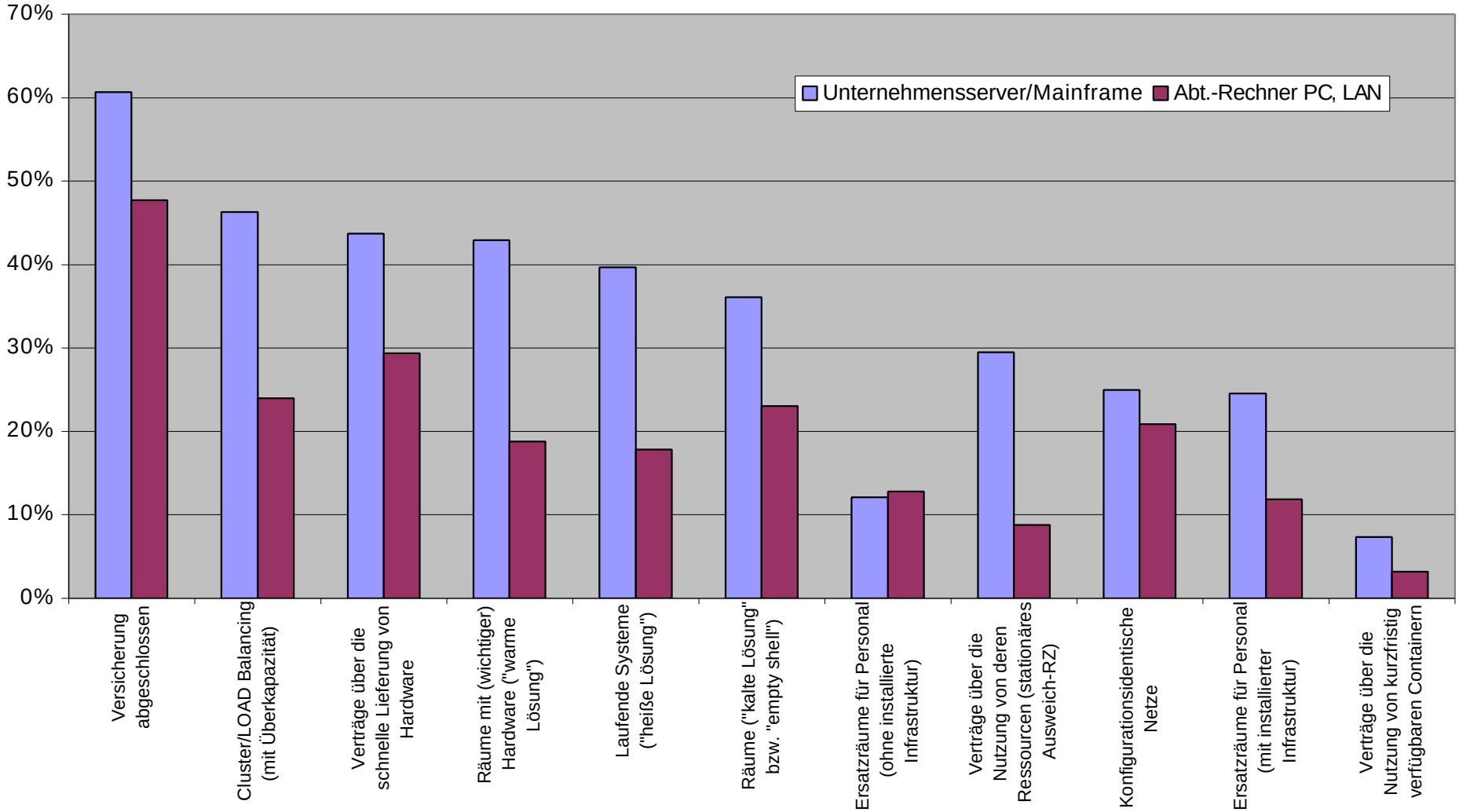
Was haben Sie für längere Ausfälle bereitgestellt? (Mehrfachnennungen möglich)

	Unternehmensserver/Mainframe			
	realisiert	geplant	nicht vorgesehen	Reihenfolge realisiert
Versicherung abgeschlossen	61%	3%	37%	1
Cluster/LOAD Balancing (mit Überkapazität)	46%	17%	37%	2
Verträge über die schnelle Lieferung von Hardware	44%	10%	47%	3
Räume mit (wichtiger) Hardware ("warme Lösung")	43%	16%	41%	4
Laufende Systeme ("heiße Lösung")	40%	10%	51%	5
Räume ("kalte Lösung" bzw. "empty shell")	36%	11%	53%	6
Ersatzräume für Personal (ohne installierte Infrastruktur)	12%	13%	75%	7
Verträge über die Nutzung von deren Ressourcen (stationäres Ausweich-RZ)	30%	15%	56%	8
Konfigurationsidentische Netze	25%	6%	69%	9
Ersatzräume für Personal (mit installierter Infrastruktur)	25%	8%	68%	9
Verträge über die Nutzung von kurzfristig verfügbaren Containern	7%	10%	83%	11
Nichts	84%	16%	0%	

	Abt.-Rechner PC, LAN			
	realisiert	geplant	nicht vorgesehen	Reihenfolge realisiert
Versicherung abgeschlossen	48%	3%	49%	1
Verträge über die schnelle Lieferung von Hardware	29%	12%	58%	2
Cluster/LOAD Balancing (mit Überkapazität)	24%	5%	71%	3
Räume ("kalte Lösung" bzw. "empty shell")	23%	9%	68%	4
Konfigurationsidentische Netze	21%	6%	73%	5
Räume mit (wichtiger) Hardware ("warme Lösung")	19%	8%	73%	6
Laufende Systeme ("heiße Lösung")	18%	6%	76%	7
Ersatzräume für Personal (ohne installierte Infrastruktur)	13%	6%	81%	8
Ersatzräume für Personal (mit installierter Infrastruktur)	12%	9%	79%	9
Verträge über die Nutzung von deren Ressourcen (stationäres Ausweich-RZ)	9%	18%	74%	10
Verträge über die Nutzung von kurzfristig verfügbaren Containern	3%	10%	86%	11
Nichts	81%	19%	0%	

	Unternehmensserver/Mainframe		Abt.-Rechner PC, LAN	
	realisiert	Reihenfolge	realisiert	Reihenfolge
Versicherung abgeschlossen	61%	1	48%	1
Cluster/LOAD Balancing (mit Überkapazität)	46%	2	24%	3
Verträge über die schnelle Lieferung von Hardware	44%	3	29%	2
Räume mit (wichtiger) Hardware ("warme Lösung")	43%	4	19%	6
Laufende Systeme ("heiße Lösung")	40%	5	18%	7
Räume ("kalte Lösung" bzw. "empty shell")	36%	6	23%	4
Ersatzräume für Personal (ohne installierte Infrastruktur)	12%	7	13%	8
Verträge über die Nutzung von deren Ressourcen (stationäres Ausweich-RZ)	30%	8	9%	10
Konfigurationsidentische Netze	25%	9	21%	5
Ersatzräume für Personal (mit installierter Infrastruktur)	25%	9	12%	9
Verträge über die Nutzung von kurzfristig verfügbaren Containern	7%	11	3%	11
Nichts	84%		81%	

Bereitstellung für längere Ausfälle



5.09a

Worauf legen Sie bei einem Recovery-Partner besonderen Wert?								
	Priorität							
	Eins	Zwei	Drei	Vier	Fünf	Sechs	Sieben	Summe
Dynamische bzw. individuelle Anpassung des Partners an Unternehmensentwicklung/-wachstum	28	51	43	40	15	8	7	192
Preisnachlässe	6	20	37	30	22	34	45	194
Beratungs- und Betriebskompetenz	49	75	32	19	4	5	2	186
Reaktionszeit im K-Fall	130	34	15	7	2	2	0	190
flexible Vertragsgestaltung, z. B. kurzfristige Kündigungsmöglichkeiten	14	13	40	27	37	31	28	190
Umfassendes, in sich abgestimmtes Service-Gesamtkonzept aus einer Hand	30	66	44	16	17	13	4	190
Umfangreiches Angebot an Rechnerplattformen	11	39	31	15	42	19	33	190

	Priorität							
	Eins	Zwei	Drei	Vier	Fünf	Sechs	Sieben	
Dynamische bzw. individuelle Anpassung des Partners an Unternehmensentwicklung/-wachstum	15%	27%	22%	21%	8%	4%	4%	
Preisnachlässe	3%	10%	19%	15%	11%	18%	23%	
Beratungs- und Betriebskompetenz	26%	40%	17%	10%	2%	3%	1%	
Reaktionszeit im K-Fall	68%	18%	8%	4%	1%	1%	0%	
flexible Vertragsgestaltung, z. B. kurzfristige Kündigungsmöglichkeiten	7%	7%	21%	14%	19%	16%	15%	
Umfassendes, in sich abgestimmtes Service-Gesamtkonzept aus einer Hand	16%	35%	23%	8%	9%	7%	2%	
Umfangreiches Angebot an Rechnerplattformen	6%	21%	16%	8%	22%	10%	17%	

5.09b

Was glauben Sie, in welchem Verhältnis steht die monatliche Vorhaltegebühr an einen Recovery-Partner zu den Investitionen für ein eigenes Ausweichrechenzentrum?		
	Nennungen	Prozentual
weniger als 1 %	38	19%
1-5 %	133	65%
mehr als 5%	34	17%
Summe	205	

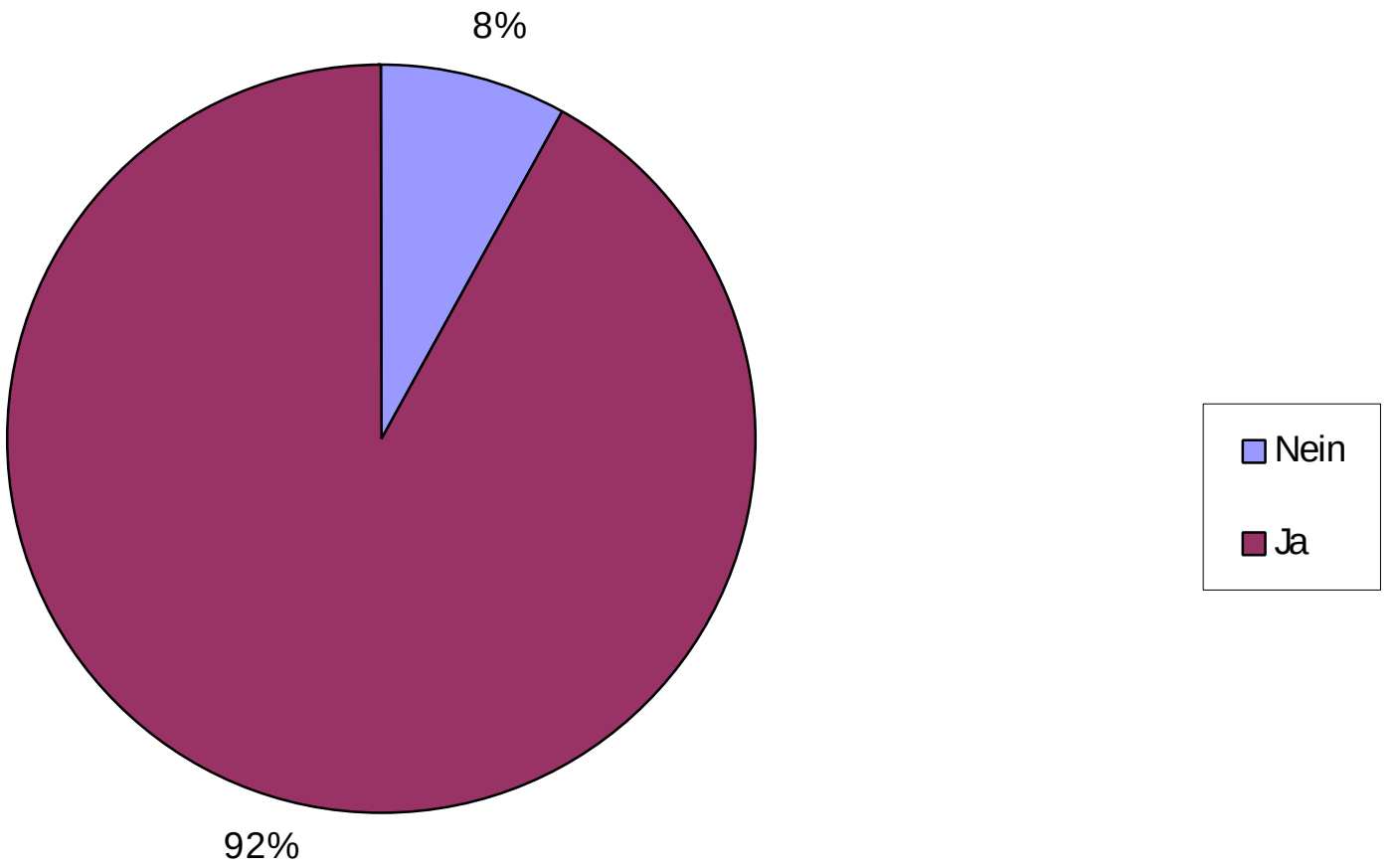
5.09d

Halten Sie es für notwendig, vor einer Entscheidung über Recovery-Maßnahmen ein strategisches Konzept zu erstellen?		
Basis der Prozentuierung Ja/Nein:	252	
	Nennungen	%
Nein	20	8%
Ja	232	92%

Durchführung mit eigenen Kräften	126	54%
mit externer Beratung	154	66%
mit Einbindung der Geschäftsführung	142	61%

Keine Angaben: 8

Strategisches Konzept als Entscheidungsgrundlage für Recovery-Maßnahmen



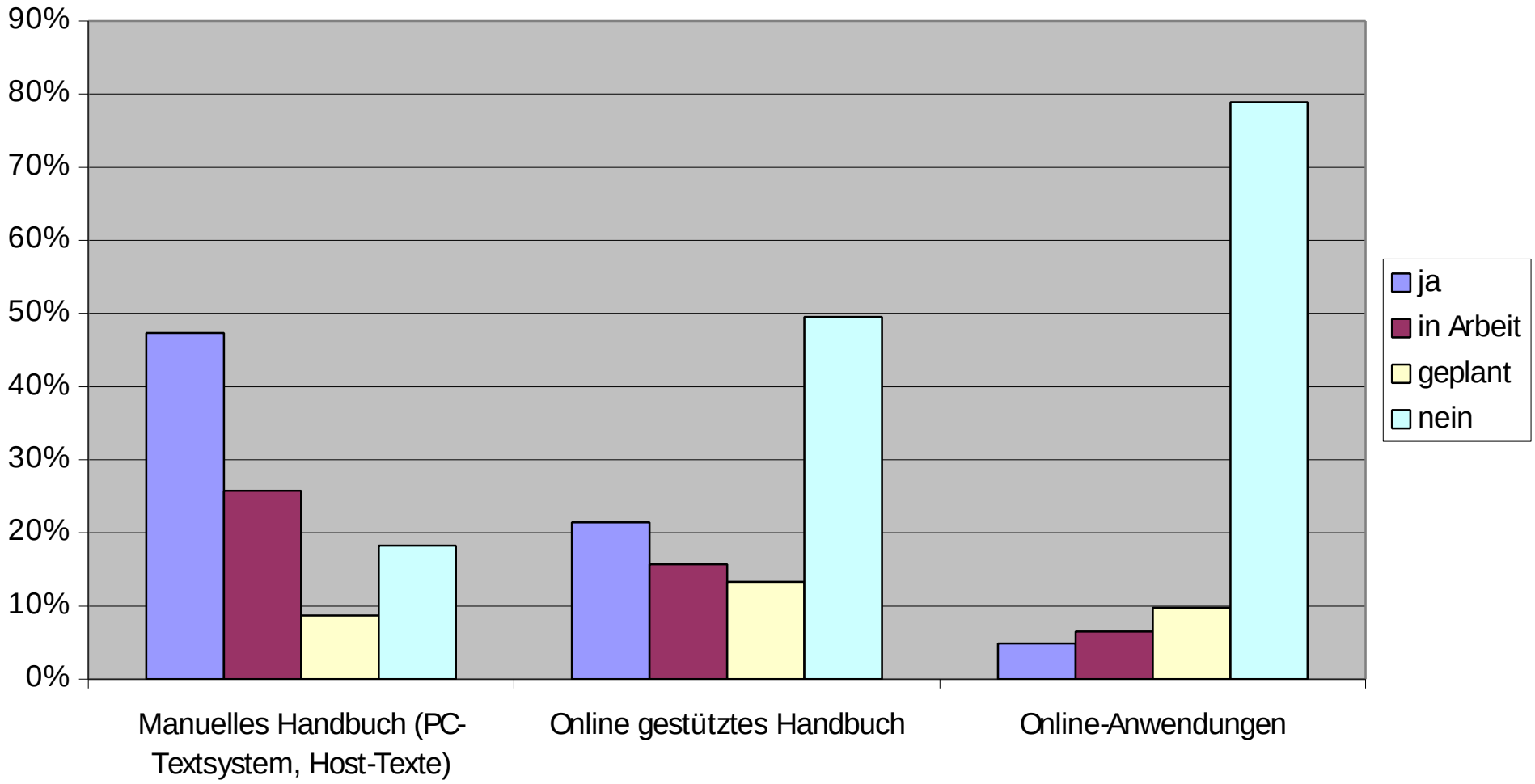
5.10

Existiert in Ihrem Hause eine Notfalldokumentation? (Mehrfachnennungen möglich)					
	ja	in Arbeit	geplant	nein	Summe
Manuelles Handbuch (PC-Textsystem, Host-Texte)	114	62	21	44	241
Online gestütztes Handbuch	45	33	28	104	210
Online-Anwendungen	9	12	18	146	185
Summe	168	107	67	294	

Es existiert min. 1 Notfalldokumentation (min. 1 x "ja")	Es existiert keine Notfalldokumentation (nur nein)
131	40

	Prozentual			
	ja	in Arbeit	geplant	nein
Manuelles Handbuch (PC-Textsystem, Host-Texte)	47%	26%	9%	18%
Online gestütztes Handbuch	21%	16%	13%	50%
Online-Anwendungen	5%	6%	10%	79%

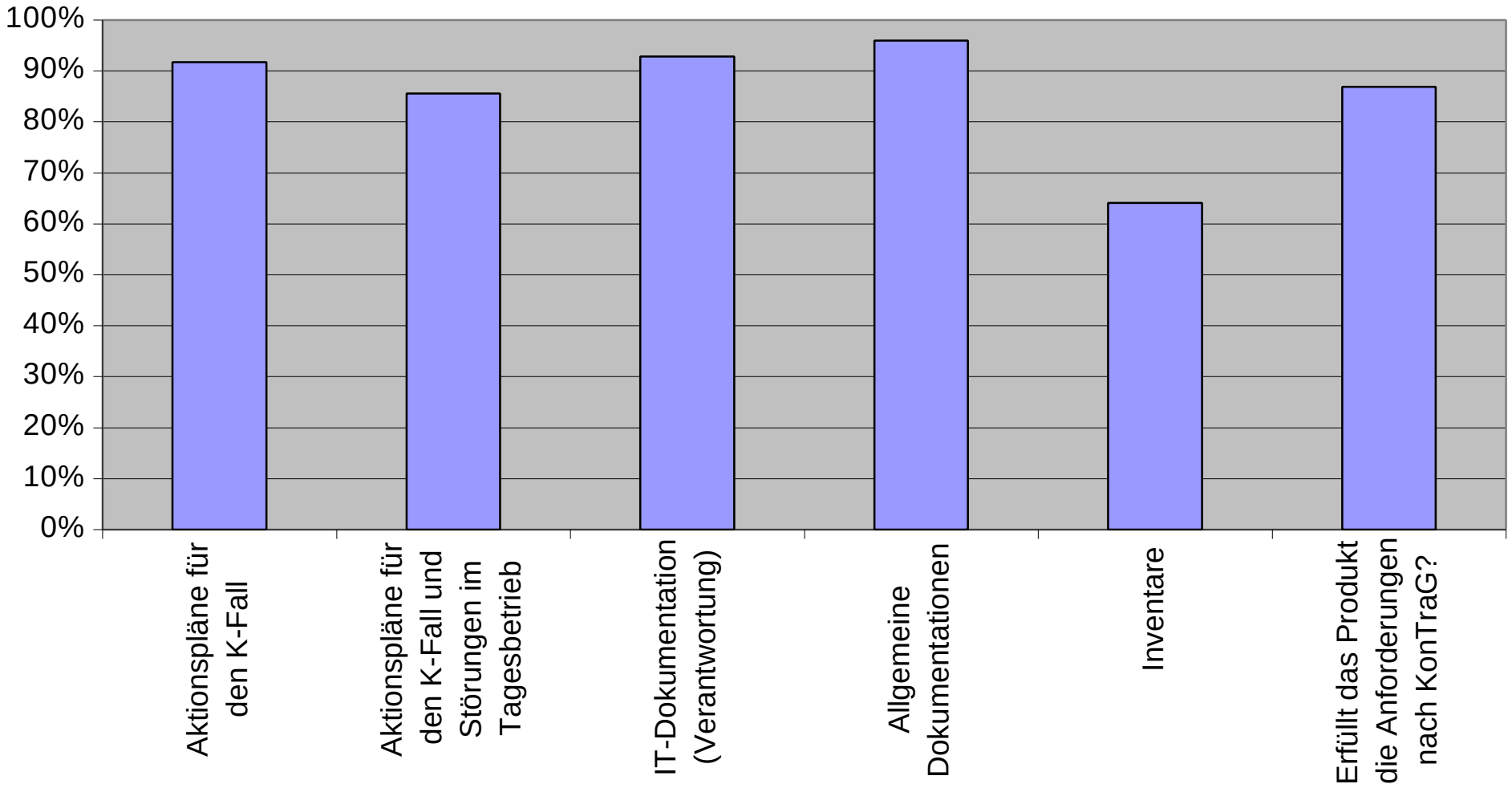
Art der Notfall-Dokumentation



5.10a

Was umfasst diese Dokumentation?						
	Ja	Nein	Summe		Ja	Nein
Aktionspläne für den K-Fall	166	15	181	Aktionspläne für den K-Fall	92%	8%
Aktionspläne für den K-Fall und Stärungen im Tagesbetrieb	148	25	173	Aktionspläne für den K-Fall und Stärungen im Tagesbetrieb	86%	14%
IT-Dokumentatin (Verantwortung)	182	14	196	IT-Dokumentatin (Verantwortung)	93%	7%
Allgemeine Dokumentationen	190	8	198	Allgemeine Dokumentationen	96%	4%
Erfüllt das Produkt die Anforderungen nach KonTraG?	139	21	160	Erfüllt das Produkt die Anforderungen nach KonTraG?	87%	13%
Inventare	50	28	78	Inventare	64%	36%

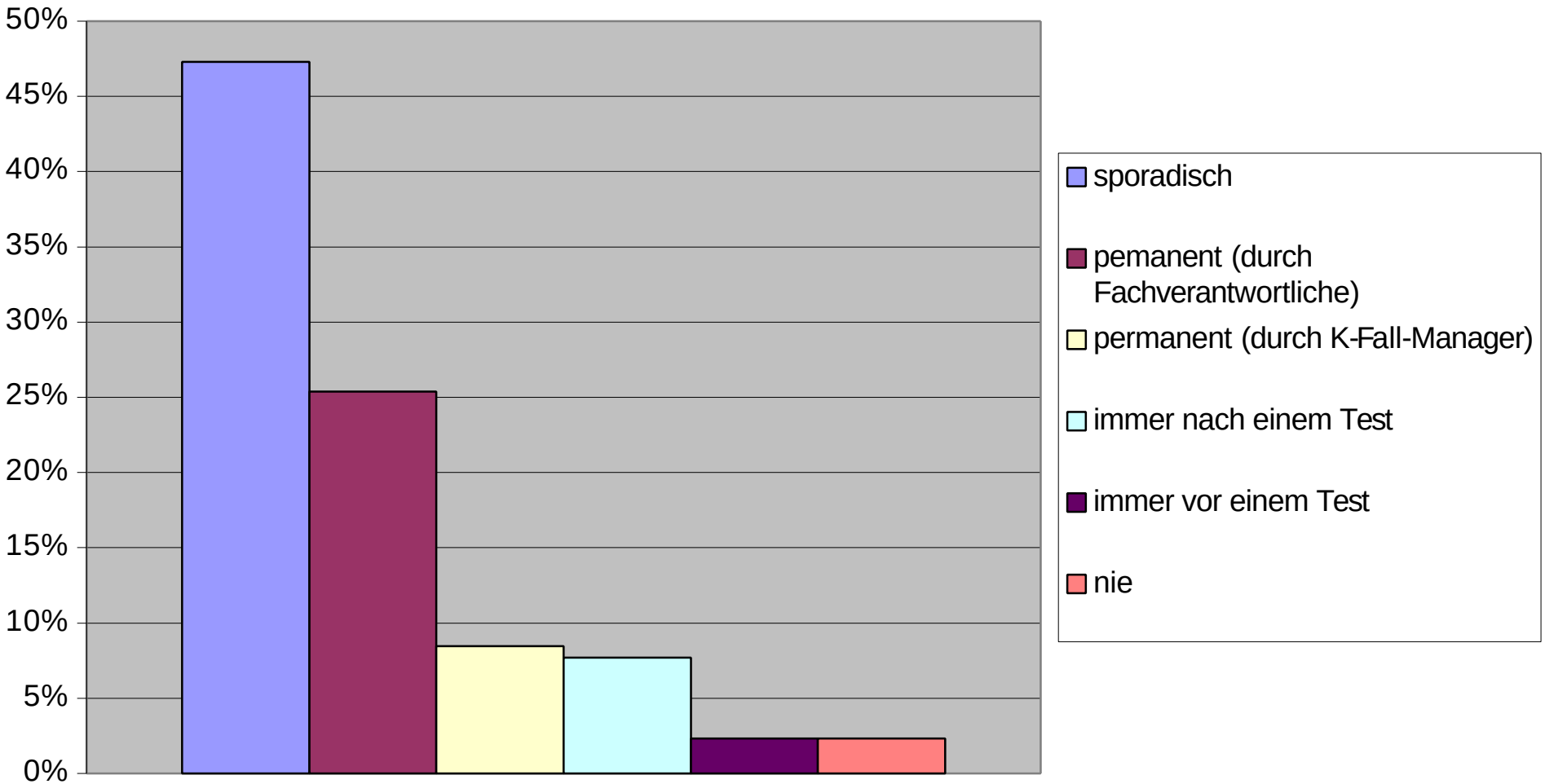
Inhalte der Notfall-Dokumentation



5.10b

Wie oft wird die Dokumentation aktualisiert?		
	Nennungen	%
sporadisch	123	47%
pemanent (durch Fachverantwortliche)	66	25%
permanent (durch K-Fall-Manager)	22	8%
immer nach einem Test	20	8%
automatisiert	8	8%
immer vor einem Test	6	2%
nie	15	3%
Summe	260	

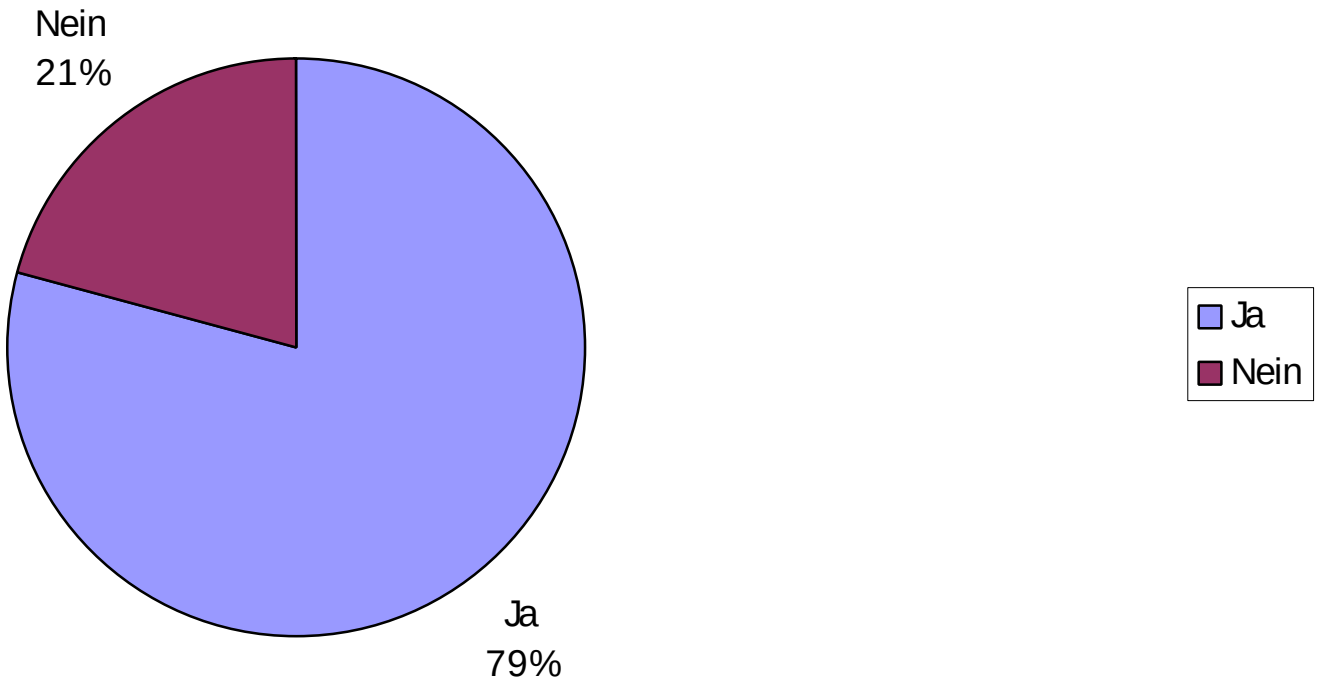
Aktualisierung der Dokumentation



5.10c

Glauben Sie, dass eine gesicherte Aktualität der gesamten Dokumentation durch den Einsatz im Tagesbetrieb erreichbar oder verbesserbar ist?			
	Ja	Nein	Summe
	194	51	245
	79%	21%	

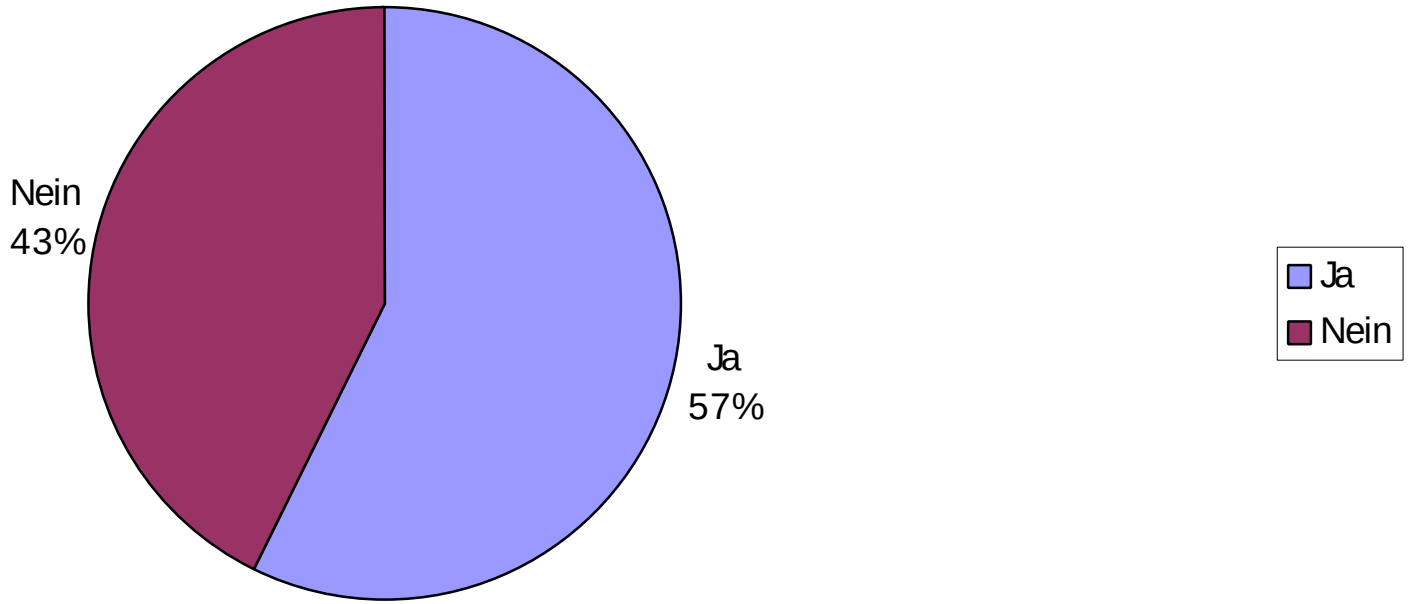
Verbesserung im Tagesbetrieb - Aktuelle Dokumentation



5.10d

Sehen Sie einen Einsatz, das Dokumentationssystems auch für den Tagesbetrieb zu nutzen?			
	Ja	Nein	Summe
	143	107	250
	57%	43%	

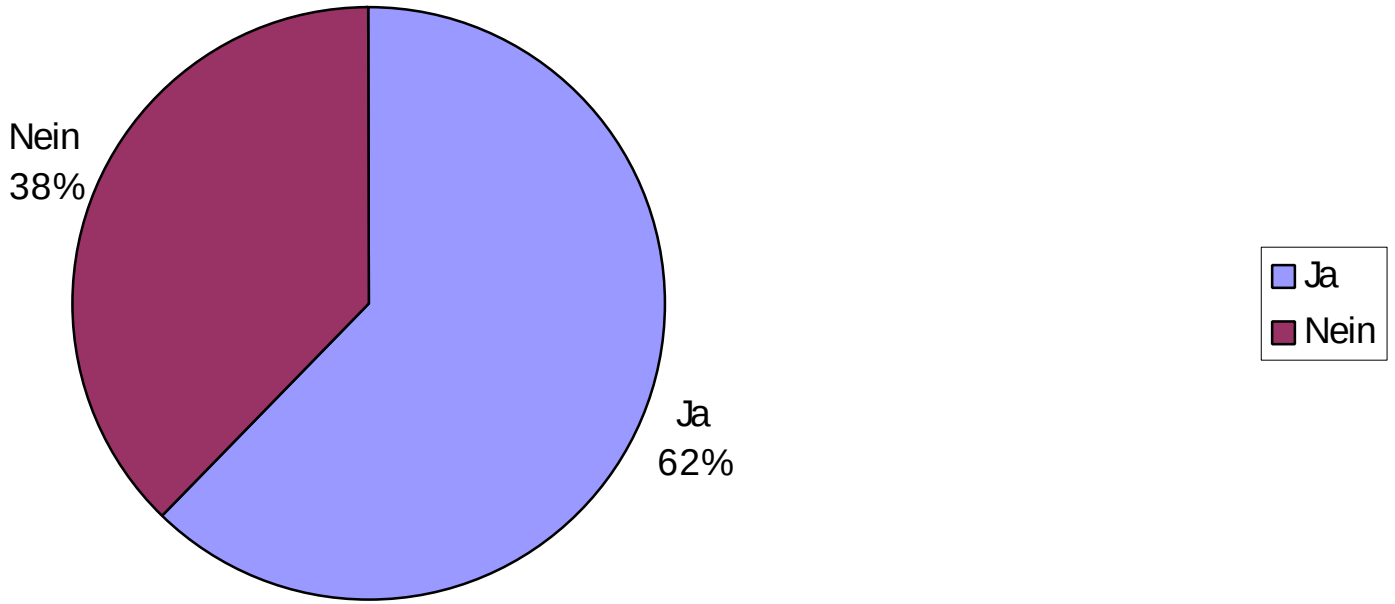
Nutzbarkeit des Dokumentationssystems für den Tagesbetrieb



5.10e

Gibt es eine verantwortliche Person für die Erstellung und Koordinierung der Notfallplanung?			
	Ja	Nein	Summe
	157	95	252
	62%	38%	

Verantwortliche Person - Erstellung/ Koordinierung Notfallplanung

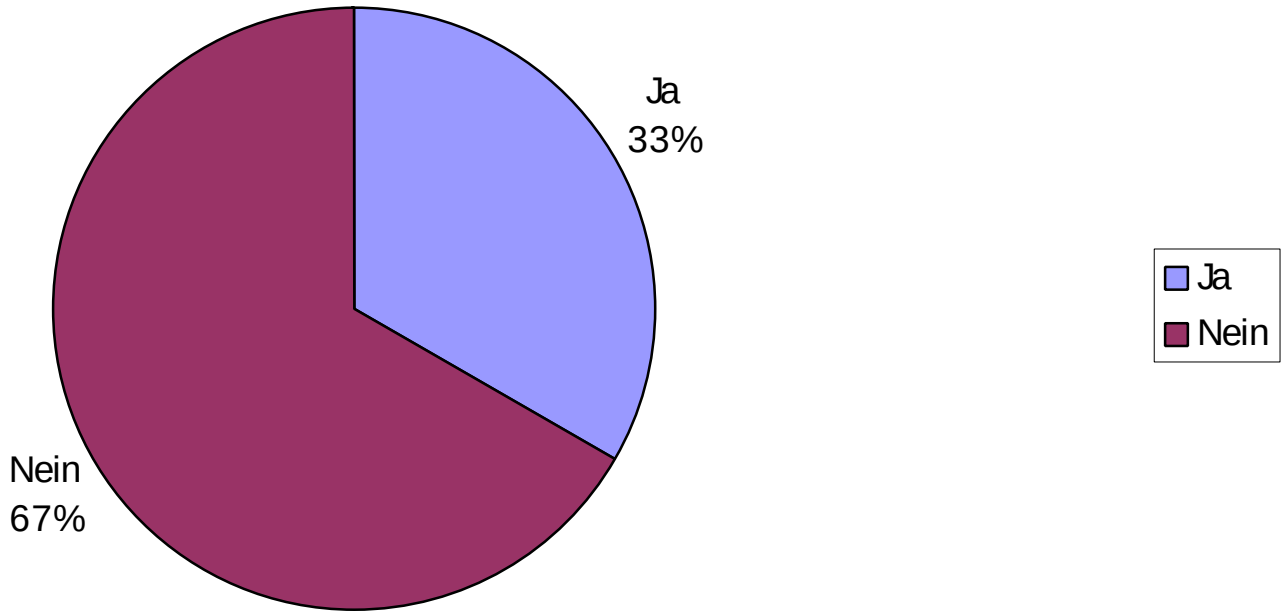


5.10f

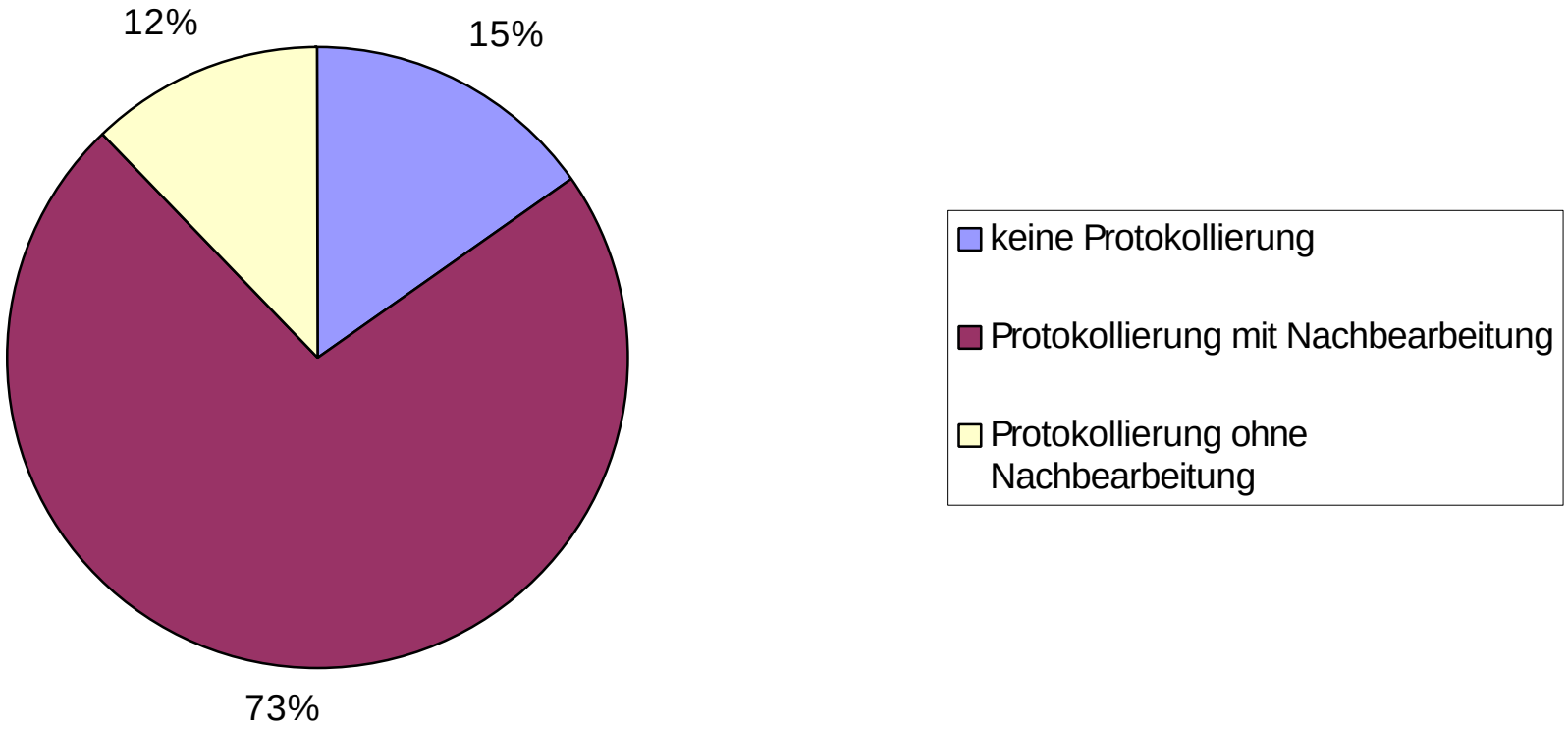
Werden Notfallübungen anhand der Dokumentation durchgeführt?			
	Ja	Nein	
	66	132	198
	33%	67%	

	Nennungen	Prozent
keine Protokollierung	10	15%
Protokollierung mit Nachbearbeitung	48	73%
Protokollierung ohne Nachbearbeitung	8	12%
Summe	66	

Durchführung von Notfallübungen - anhand der Dokumentation



Protokollierung mit/ ohne Nachbearbeitung oder keine Protokollierung

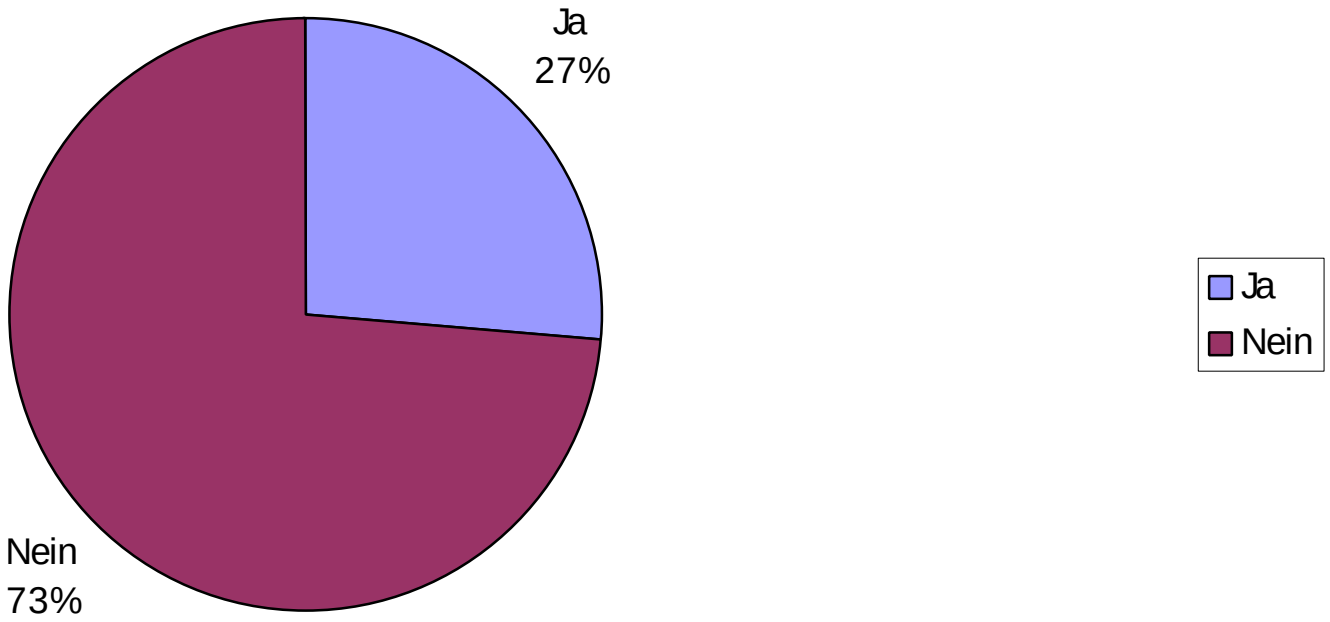


5.10g

Wurden bereits Störfälle auf Basis der Dokumentation bearbeitet?			
	Ja	Nein	Summe
	66	183	249
	27%	73%	

Keine Angaben: 11

Bearbeitung von Störfällen - auf Basis der Dokumentation



5.11

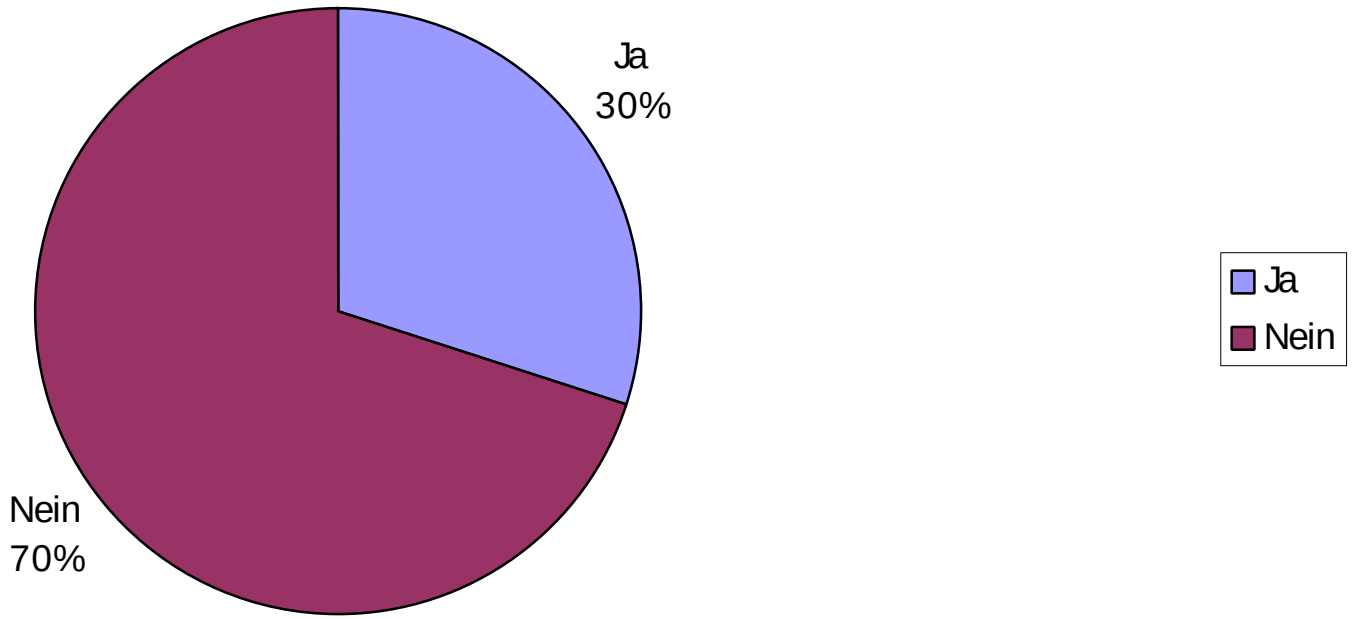
Haben Sie in Ihrem Sicherheitskonzept physische Risiken bewertet und berücksichtigt?			
	Ja	Nein	Summe
	70	164	234
	30%	70%	

Keine Angaben: 26

Welche Vorgaben/Normen werden beachtet:

	Nennungen
Euronorm 1047-1	2
Euronorm 1047-2	0
Baunorm DIN 4102	15
NFPA-Vorschriften	2
UL-Standards	0
keine	46

Berücksichtigung von pyhsischen Risiken im Sicherheitskonzept

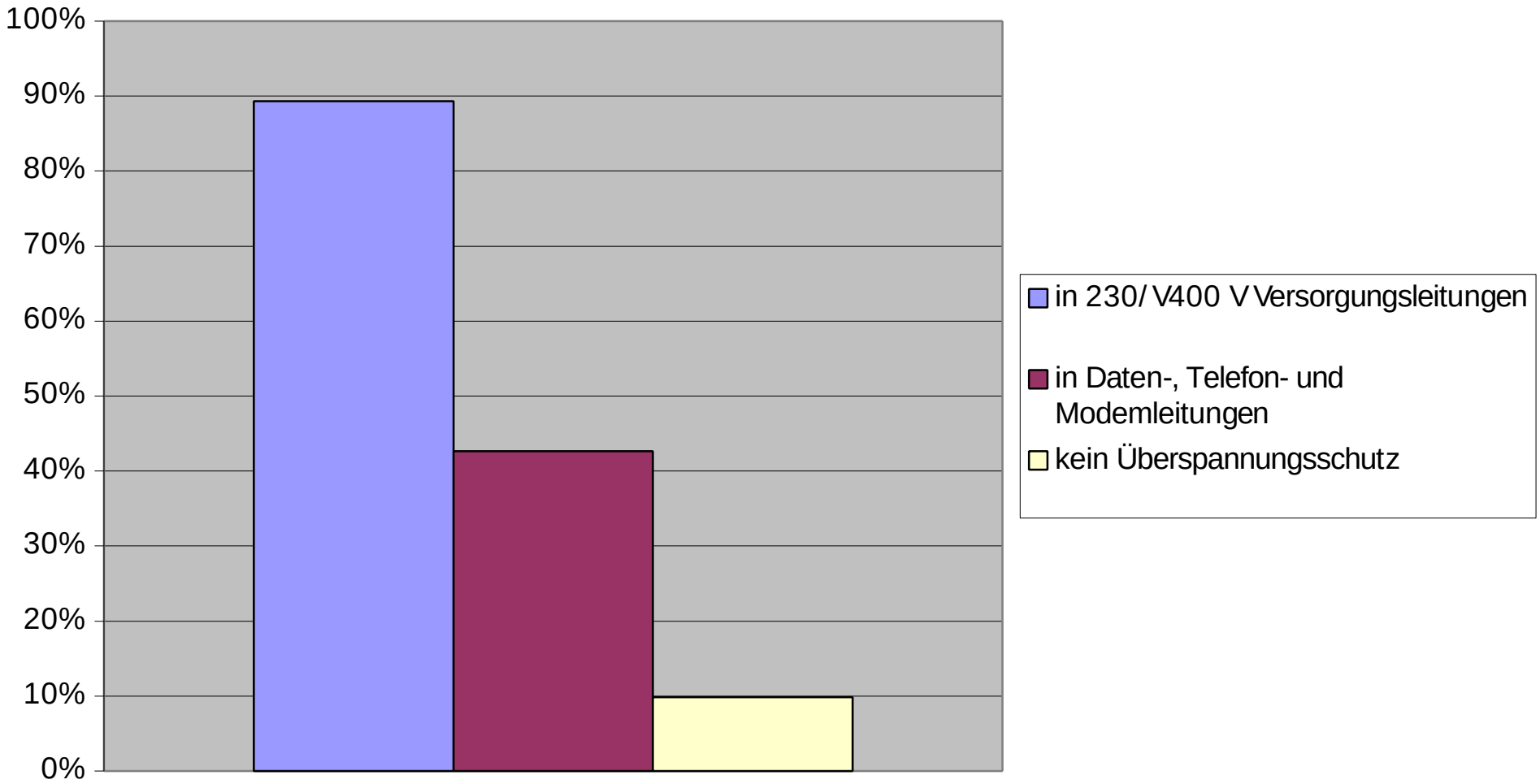


5.12

Ist Ihre EDV mit Überspannungsschutzbausteinen ausgerüstet? (Mehrfachnennugnen möglich)		
Basis der Prozentuierung:	244	
	Nennungen	%
in 230/V400 V Versorgungsleitungen	218	89%
in Daten-, Telefon- und Modemleitungen	104	43%
kein Überspannungsschutz	24	10%

Keine Angaben: 16

Überspannungsschutzbausteine

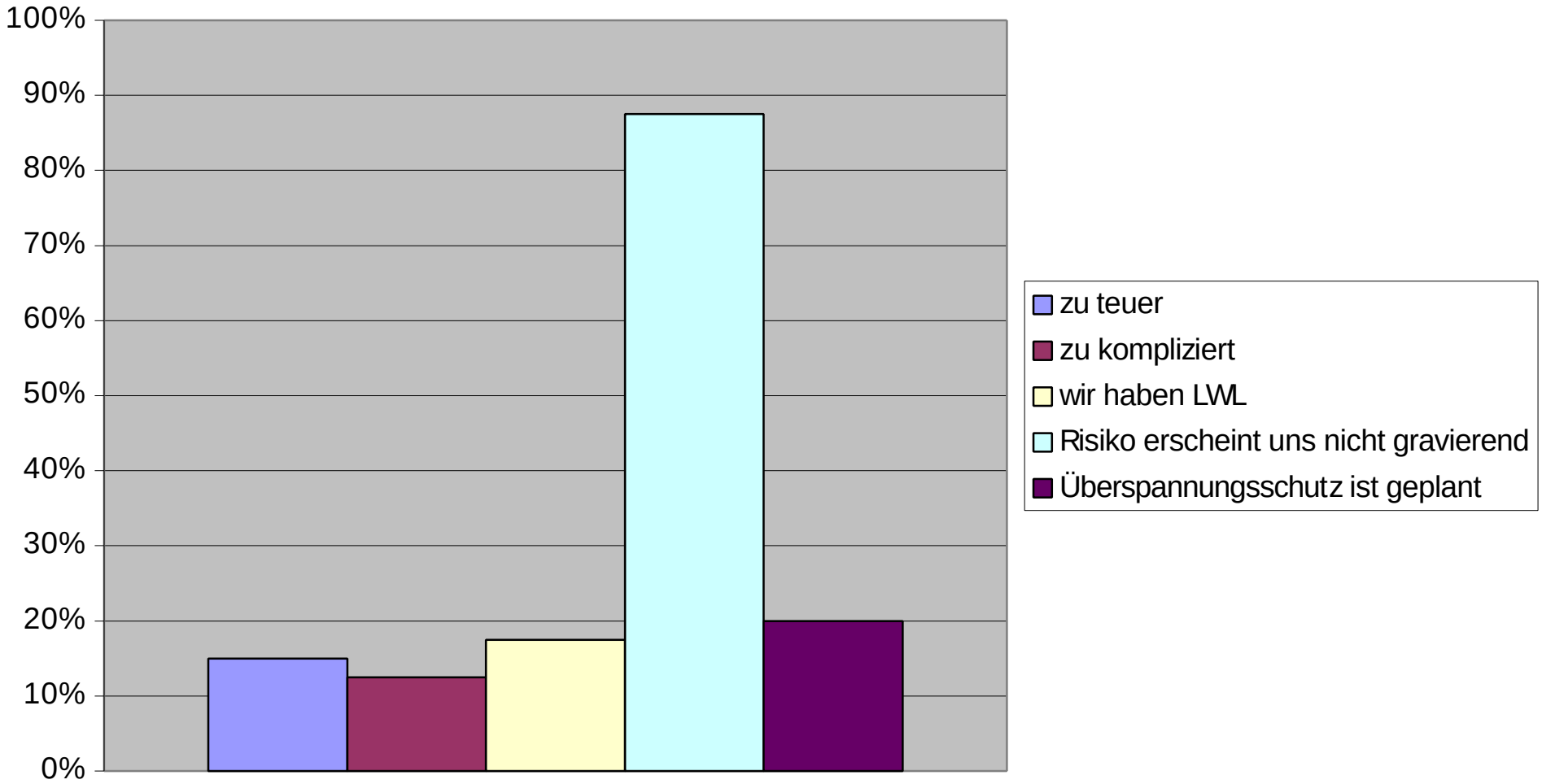


5.12a

Wenn kein Überspannungsschutz vorhanden ist: Was sind die Gründe? (Mehrfachnennungen möglich)		
Basis der Prozentuierung:	40	(Zusammenstehend aus 24 Nennungen die kein Überspannungsschutz angekreuzt haben und 16 die keine Angaben gemacht haben)

	Nennungen	%
zu teuer	6	15%
zu kompliziert	5	13%
wir haben LWL	7	18%
Risiko erscheint uns nicht gravierend	35	88%
Überspannungsschutz ist geplant	8	20%

Kein Überspannungsschutz - Gründe



5.13

Welche der folgenden Unternehmen, die Sicherheitsprodukte anbieten, sind Ihnen bekannt? (Mehrfachnennungen möglich)		
Basis der Prozentuierung:	252	
	Nennungen	Prozentual
Symantec	204	81%
Network Associates (NAI)	185	73%
RSA Security	172	68%
Utimaco Safeware	171	68%
TrendMicro	161	64%
Integralis	131	52%
iT_SEC	127	50%
Sophos	122	48%
Norman Data Defense Systems	114	45%
Ontrack	113	45%
Entrust	101	40%
Baltimore	97	38%
Rohde & Schwarz SIT	84	33%
accent Technologies	76	30%
Secude	66	26%
GeNUA	51	20%
Rainbow	47	19%
Allasso	45	18%
In der Liste fehlen:	41	16%
Algorithmic Research	36	14%
Qualys	20	8%
Adolphs	18	7%
Adiva	17	7%
Faktum	16	6%
Astrum	10	4%
Keine Angaben:	8	

Produkte die als fehlent genannt wurden:	Checkprint, Stone Beat, Argus-Systems, Real Secounouia, Secur ID, Vasco, Biometrics, F-Secure, Heine & Partner, AVP/ Kaspersky Group (Notes-Lösungen), ROG, Checkpoint, Nokia, CA, Checkpoint, Cisco, Axent, IHFO AG, Lampertz, Sybaris, secunet, H+B EDV, Group-Technologies, chekpoint, ISS, Finjan, HiSoluti-ons, TÜV secure IT