Lagebericht zur Informations-Sicherheit (3)

Verlässliche Zahlen zur Informations-Sicherheit (ISi) findet man nur selten. Noch seltener sind konkrete Angaben zu Schäden und Budgets sowie selbstkritische Bestandsaufnahmen zur Sicherheitslage. In diesem Jahr haben erneut über 160 Teilnehmer den <kes>-Fragebogen als Checkliste für ihre eigene Sicherheit genutzt und damit gleichzeitig wertvolle Daten geliefert.

Die vertrauensvollen und umfassenden Antworten der Teilnehmer und die Unterstützung der Sponsoren und Partner machen diese Studie möglich – dafür zunächst vielmals Dankeschön! In diesem Jahr sind 163 ausgefüllte Fragebögen eingegangen. Dabei war auch eine erfreulich hohe Beteiligung durch kleine und mittelständische Unternehmen (KMU) mit bis zu 500 Mitarbeitern zu verzeichnen. Die ersten beiden Teile der Ergebnisse sind bereits in <kes> 2006#4 und <kes> 2006#5 erschienen; wichtige Kernpunkte dieses dritten Teils der Auswertung lauten:

_____ Mangelnde Sicherheitsmaßnahmen bei mobilen Endgeräten: über ein Fünftel ungeschützt gegen Malware, fast 60 % derzeit ohne Datensicherung

_____ Open-Source-Software bei 68 % im Einsatz – hauptsächlich aus Kostengründen

_____ Multi-Vendor-Strategien überwiegen bei der Virenabwehr: 59 % nutzen aus Sicherheitsgründen Lösungen von zwei oder mehr Anbietern

Maßnahmen

Die „große Maßnahmen-Checkliste“ (Tab. 1) belegt wie üblich eine eher serverzentrische Sicherheitsorganisation: Zum Client oder mobilen Endgerät hin nimmt der Umsetzungsgrad der meisten Sicherheitsmaßnahmen ab. Als heikel könnten sich dabei einige fehlende Schutzmechanismen bei mobilen Endgeräten erweisen, die auch die unbefriedigende Sicherheitseinschätzung dieser Systeme untermauert: Über ein Fünftel der mobilen Endgeräte ist derzeit (noch) ungeschützt gegen Malware; 13 % gaben sogar an, dass ein Virenschutz dort auch künftig nicht vorgesehen ist. (Personal) Firewalls sind ebenfalls noch selten: Bei 21 % der Studienteilnehmer ist diese Maßnahme geplant, aber noch nicht realisiert – 37 % wollen *keine* „mobilen Firewalls“ einrichten. Und fast 60 % betreiben derzeit keine Datensicherung für mobile Systeme.

Eine Besserung ist bei der kryptographischen Sicherung von WLANs zu beobachten: Der Anteil der „Nicht-Verschlüssler“ ist um rund zehn Prozentpunkte zurückgegangen, allerdings mit nach wie vor über 50% der Teilnehmer immer noch recht hoch. Bei Voice-over-IP planen noch erheblich mehr Organisationen, auf Verschlüsselung völlig zu verzichten – immerhin liegen die entsprechenden Werte unter denen der „klassischen“ Telefonie.

Waren 2004 noch etliche Maßnahmen zur Spam-Abwehr in Planung, so sind diese nunmehr größtenteils umgesetzt – gut so, denn der mittlere Spam-Anteil ist heuer um gut acht Prozentpunkte auf 33 % gestiegen (vgl. Abb. 1). Weiterhin auf vielen „to-do“-Listen stehen Intrusion-Detection/Prevention-Systeme; ebenfalls erhebliches Planungspotenzial zeigen Benutzerverzeichnisse mit Security-Policy, Langzeitarchivierung, Schnittstellen-überwachung (USB, Bluetooth usw.) sowie allem voran Signatur- und Verschlüsselungsmaßnahmen für E-Mails sowie virtuelle Poststellen (12 % realisiert, 32 % geplant). Für mobile Endgeräte plant zudem noch eine größere Zahl von Organisationen Verschlüsselungsmechanismen für Festplatten und mobile Speicher einzurichten.

Ob bei zukünftigen Anschaffungen Produkte mit einer Sicherheitszertifizierung nach anerkannten Standards bevorzugt werden, ist weiterhin bei der Mehrheit der Befragten offen (56 %) – 16 % haben sich bereits dagegen entschieden. Der Anteil der klaren Befürworter zertifizierter Sicherheitssysteme liegt heuer bei 28 % – innerhalb der Teilnehmer-Gruppe, die bereits solche Produkte im Einsatz hat (41 %), ver-

	Server / Zentrale			Clients / Endstellen			mobile Endgeräte		
	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen	realisiert	geplant	nicht vorgesehen
Firewalls	89%	6%	4%	52%	10%	38%	42%	21%	37%
Virenschutzmechanismen	94%	4%	3%	98%	1%	1%	79%	9%	13%
Datensicherung (Backup)	97%	1%	2%	50%	4%	46%	41%	6%	53%
Langzeit-Archivierung	62%	22%	16%	19%	5%	76%	14%	7%	80%
Intrusion Detection/Prevention Systems	47%	24%	29%	16%	11%	72%	13%	8%	80%
Benutzerverzeichnis mit Security Policy	57%	22%	22%	35%	15%	50%	31%	13%	56%
Authentifizierung									
... Hardware-Token	16%	7%	77%	18%	9%	72%	23%	13%	64%
... Passwort	93%	1%	6%	92%	3%	5%	82%	4%	15%
... Chipkarte	10%	13%	76%	14%	13%	73%	14%	6%	80%
... biometrische Verfahren	3%	4%	93%	5%	10%	85%	3%	8%	89%
Protokollierung unberechtigter Zugriffe	76%	13%	12%	36%	13%	51%	21%	11%	68%
Schnittstellenüberwachung/-schutz (USB, ser., par., Bluetooth, ...)	28%	22%	50%	23%	29%	48%	17%	30%	53%
Netzwerkzugangskontrolle (EAP, NAC, ...)	48%	16%	36%	22%	18%	60%	17%	15%	67%
Content Inspection/Filtering									
(Adress-/Inhaltsfilter)	56%	15%	29%	29%	13%	58%	17%	9%	74%
Spam-Abwehr	79%	13%	8%	59%	14%	27%	47%	10%	43%
Verschlüsselung									
... sensitive Daten	48%	13%	38%	34%	17%	49%	36%	16%	48%
... Festplatten (komplett/partitionsweise)	19%	17%	64%	17%	16%	67%	35%	22%	44%
... mobile Speicher (USB, Firewire, ...)	16%	14%	70%	18%	17%	65%	20%	23%	58%
... Archivdatenträger/Backups	19%	13%	68%	12%	8%	79%	9%	9%	82%
... drahtlose Peripherie (Funktastatur, Bluetooth, ...)	12%	9%	80%	13%	11%	75%	15%	10%	75%
... LAN/Intranet-Verbindungen	29%	17%	54%	23%	16%	61%	23%	9%	68%
... WLAN-Verbindungen	39%	11%	51%	31%	12%	57%	38%	10%	51%
... WAN/Internet-Verbindungen	46%	14%	40%	33%	14%	53%	38%	9%	53%
... Telefon	9%	6%	85%	8%	3%	89%	6%	2%	92%
... Voice over IP (VoIP)	11%	12%	77%	10%	12%	78%	11%	9%	80%
... Fax	8%	4%	88%	6%	2%	92%	3%	3%	94%
... E-Mail	31%	25%	45%	34%	23%	44%	32%	18%	50%
Elektronische Signaturen									
... E-Mail	26%	32%	42%	27%	33%	40%	23%	26%	51%
... Web (SSL/TLS)	48%	13%	40%	37%	19%	44%	29%	13%	58%
... Applikationen	18%	14%	69%	14%	15%	71%	13%	10%	77%
physische Sicherheit									
... Zutrittskontrolle, biometrisch	12%	5%	83%	7%	5%	89%			
... Zutrittskontrolle, sonstige	85%	3%	12%	54%	4%	43%			
... Bewachung	47%	2%	51%	25%	1%	73%			
... Video-Überwachung	38%	7%	55%	19%	1%	80%			
... Einbruchmeldeanlage	67%	7%	27%	39%	4%	58%			
... Schutz von Glasflächen gegen Durchbruch/-wurf	52%	5%	44%	22%	4%	74%			
... Sicherheitstüren	68%	6%	25%	27%	3%	71%			
... Brandmeldesysteme	81%	4%	15%	45%	1%	54%			
... Löschanlagen	54%	5%	41%	25%	1%	74%			
... andere Meldesysteme (Gas, Staub, Wasser, ...)	44%	5%	51%	11%	2%	87%			
... Datensicherungsschränke/-räume	80%	7%	13%	21%	4%	74%			
... Schutz gegen kompromittierende Abstrahlung (Tempest)	13%	4%	83%	5%	3%	92%	3%	3%	93%
... Maßnahmen gegen Hardware-Diebstahl	60%	6%	34%	36%	8%	56%	31%	13%	56%
physikalisches Löschen von Datenträgern	64%	7%	29%	50%	12%	38%	44%	12%	44%
unterbrechungsfreie Stromversorgung (USV)	90%	5%	6%	21%	5%	74%	10%	5%	85%
Überspannungsschutz für Stromleitungen	84%	5%	10%	39%	4%	56%	18%	5%	78%
Überspannungsschutz für Daten-/ TK-Leitungen	60%	7%	34%	25%	5%	70%	14%	4%	82%
Klimatisierung	85%	4%	11%	14%	1%	84%			
Rückrufautomatik bei Modemzugriff	47%	5%	48%	17%	3%	80%	10%	6%	83%
Reserve-Netzzugang (IT/TK) zur Ausfallüberbrückung	53%	15%	32%	18%	9%	73%	13%	5%	82%

Basis: Ø 147 Antworten (Server), Ø 138 (Clients), Ø 133 (mob. Endgeräte)

Tabelle 1 Realisierte und geplante Sicherheitsmaßnahmen

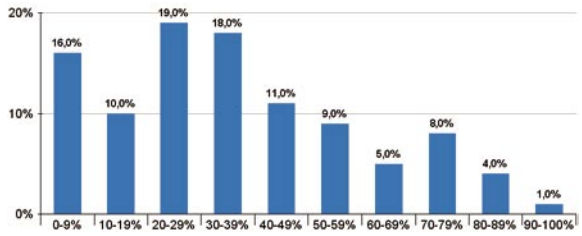

Abbildung 1: Anteil von Spam an der eingehenden E-Mail

Basis: 147 Antworten

doppelt er sich jedoch fast. Immerhin gaben auch 69 % an, ihre Erwartungen an Nutzen und Zuverlässigkeit dieser Systeme hätten sich erfüllt. Einen höheren Preis zertifizierter Produkte hielten insgesamt 50 % für gerechtfertigt. Zur Bekanntheit und Bedeutung verschiedener ISi-Kriterienwerke siehe Abbildung 2.

Tabelle 2: Realisierte und geplante PKI-Funktionen

PKI-Funktionen	realisiert	geplant	nicht vorgesehen
E-Mail-Verschlüsselung	41%	43%	16%
Dateiverschlüsselung	27%	41%	32%
Zugriffsrechte	17%	33%	49%
Single-Sign-On	17%	34%	49%
Virtual Private Networks	30%	30%	39%
Telearbeitsplätze / Remote Access	31%	29%	40%
Web-Zugriff	18%	30%	52%

Basis: Ø 89 Antworten

Tabelle 3: Hemmnisse für den Einsatz von Identity-Management

	sehr problematisch	problematisch	unproblematisch
technische Komplexität/ aufwändige Einführung	37%	51%	12%
organisatorische Komplexität/ aufwändige Einführung	38%	48%	14%
ROI schwer berechenbar/ nachvollziehbar	35%	44%	21%
hohe Produktkosten	29%	43%	28%
hohe Betriebskosten	23%	45%	32%
Herstellerabhängigkeit	22%	38%	41%

Basis: Ø 77 Antworten

Tabelle 4: Realisierte und geplante Infrastruktur für elektronische Signaturen

Folgende Infrastruktur ist ...	realisiert	geplant	nicht vorgesehen
nur Software	44%	15%	41%
Hardwaremodule	2%	8%	89%
Hardware-Token	10%	15%	75%
Chipkarten	20%	18%	62%
Klasse-2-Chipkartenterminal (sichere PIN-Eingabe)	12%	13%	75%
Klasse-3-Chipkartenterminal (mit eigenem Display)	7%	7%	85%
gemäß Signaturgesetz (SigG)			
... fortgeschrittene Signatur	22%	17%	61%
... qualifizierte Signatur	18%	24%	59%
... qualifizierte Signatur mit Anbieterakkreditierung	9%	16%	75%
nichts von alledem	24%	17%	

Basis: Ø 96 Antworten

PKI und IDM

Als Dauer-Investitionsvorhaben erweisen sich Public-Key-Infrastrukturen (PKI): Weiterhin plant ein Drittel der Studienteilnehmer die Einrichtung einer PKI, aber nur ein gutes Viertel aller Befragten hat solche Pläne bereits umgesetzt – die vorgesehenen Einsatzzwecke nennt Tabelle 2. Noch eine richtige Seltenheit sind realisierte Identity-Management-Systeme (IDM) – bei nur 5 % der Befragten. 22 % planen für die Zukunft ein IDM. Die vorgesehenen Hauptziele dafür wären dann die Realisierung einer konsistenten Rechtevergabe, Sicherheitsgewinne durch Policy-Enforcement und eine bessere Revisionierbarkeit. Kostenersparnisse erwartet kaum jemand, dafür jedoch viele Probleme bei der Einrichtung: Nur 12 % beziehungsweise 14 % sehen die technische beziehungsweise organisatorische Komplexität eines IDM als unproblematisch an (vgl. Tab. 3).

Virtual Private Networks (VPNs)

Das verbreitetste VPN-Verfahren bleibt IPsec: 74 % haben bereits mindestens ein IPsec-VPN realisiert, weitere 9 % planen dies. Doch auch SSL-VPNs sind bereits bei 58 % im Einsatz und bei 13 % in Planung. Die weitaus meisten Studienteilnehmer (73 %) sehen keine grundsätzlichen Argumente gegen SSL-VPNs – 14 % gaben indes an, diese Variante decke sich nicht mit bestehenden Anforderungen, 8 % hatten Vorbehalte wegen der Kosten und 3 % äußerten, es fehle an einer passenden Lösung.

E-Mail-Verschlüsselung

Auch in diesem Jahr lässt sich eine leichte Steigerung der Bereitschaft erkennen, E-Mails verschlüsselt zu senden, sofern ein Krypto-Schlüssel des Empfängers verfügbar ist: Der Anteil derer, die dennoch *nicht* verschlüsseln würden, sank um zwei Prozentpunkte auf 42 % – gleichzeitig stieg die Zahl der Befragten, die dann alle externen (13 %) oder sogar generell alle Nachrichten verschlüsseln würden (8 %). Erneut gaben 47 % an, zumindest sensitive Mails zu chiffrieren (Mehrfachnennungen). Klar aufgeholt hat dabei S/MIME: (Open)PGP liegt zwar mit 66 % Nutzung immer noch vorn, die Zahl der (zumindest auch-) S/MIME-Anwender stieg aber sprunghaft auf 57 % (2004: 34 %).

Elektronische Signaturen

Klar an erster Stelle bei elektronischen Signaturen liegen weiterhin reine Softwarelösungen, die allerdings auch nur 44 % der Befragten bereits nutzen (vgl. Tab. 4 – zu den Einsatzzwecken vgl. Tab. 1). Eine gewisse Steigerung des Interesses scheint bei den weniger streng reglementierten Varianten gemäß Signaturgesetz (SigG) vorzuliegen: Lösungen für fortgeschrittene und

qualifizierte Signaturen (ohne Anbieterakkreditierung) gaben jeweils rund ein Fünftel der Befragten als bereits realisiert an – nur noch etwa 60 % erteilen diesen eine pauschale Absage. Bei qualifizierten Signaturen mit Anbieterakkreditierung bleibt jedoch weiterhin eine große Zurückhaltung festzustellen, die zu weniger als zehn Prozent bestehender Umsetzung und 75 % dauerhafter Ablehnung führt.

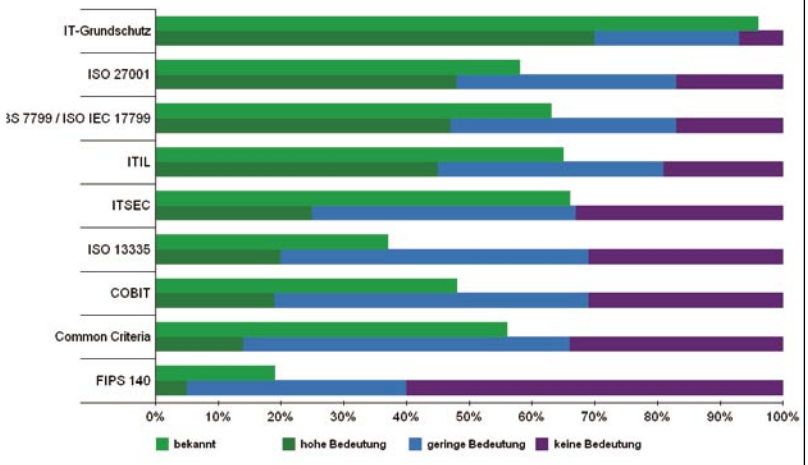

Abbildung 2: Bekanntheit und praktische Bedeutung von ISi-Kriterienwerken

Basis: Ø 138 Antworten (Bekanntheit), 141 (Bedeutung Grundschutz), Ø 84 (Bedeutung andere)

Vielen Dank für freundliche Unterstützung unserer Studie

Microsoft
ASTRUM IT
itWatch GmbH
ROG
BorderWare
Jürgen Jakob Software-Entwicklung
SAP
AVG Anti-Virus
TRUST
PGP
»|secaron e.security solutions
entrada IT-Security
phion
SONICWALL
Kroll Ontrack
ibas VOGON
UNTERNEHMEN DER KROLL ONTRACK GMBH
it.sec security for your information
proRZ professioneller Rechenzentrumsbau
TESIS SYSware

Für zusätzliche Anregungen und Hinweise bedanken wir uns beim Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie bei der Hans-Joachim Gaebert Unternehmensberatung. Weiterhin gilt unser Dank den Verbänden und Anwendervereinigungen, die den Fragebogen der Studie ihren Mitgliedern zugänglich machen, sowie schon jetzt allen Teilnehmern an der Befragung, die durch ihre wertvolle Mitarbeit ein sinnvolles Gesamtbild entstehen lassen.

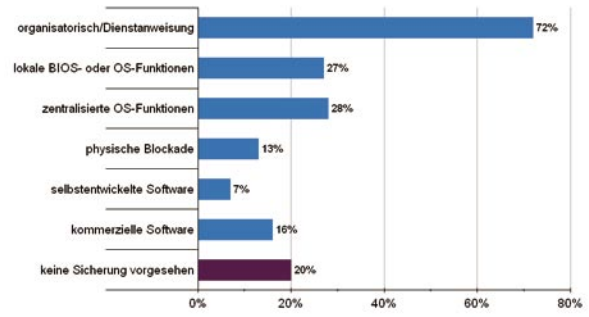

Abbildung 4: Mechanismen zur Schnittstellen-Sicherung (USB, seriell, parallel usw.)

Basis: 158 Antworten

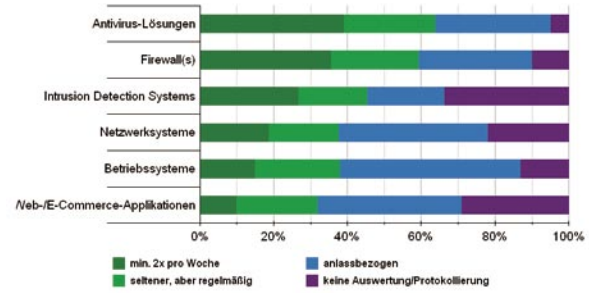

Abbildung 5: Auswertung von Log-Daten

Basis: Ø 149 Antworten

Im Einsatz sind Lösungen von ...	einem Anbieter	zwei Anbietern	drei und mehr Anbietern
Anti-Virus-Software	41%	42%	17%
Firewalls	59%	35%	6%
Router	61%	27%	13%
Server-Betriebssysteme	47%	36%	18%
Web-Server	63%	30%	7%
Applikation-Server	55%	26%	19%

Tabelle 5: Heterogenität aus Sicherheitsgründen (Multi-Vendor-Strategie)

Basis: Ø 144 Antworten

Viren-Scanner	Update-Frequenz [Std.]
an der Firewall/Internet-Gateway	14,5
auf dem Mail-/File-/Applikationsserver	13,3
auf den PCs/Workstations	23,9
auf mobilen Systemen	40,6

Tabelle 6: Updatefrequenz von Viren-Scannern (Mittelwert)

Basis: Ø 104 Antworten (mob. Systeme: 81)

Open-Source-Software

Der Anteil der Studienteilnehmer, die Open-Source-Software (OSS) für sicherer halten als Programme mit nicht-offengelegtem Quellcode, ist im Vergleich zu 2004 um sechs Prozentpunkte gesunken – gleichzeitig verbuchten die ausgesprochenen Kritiker Zuwachs (s. Abb. 3). Dennoch ist OSS bei 68 % der Studienteilnehmer im Einsatz, und zwar weiterhin überwiegend aus Kostengründen (50 %) statt aus Sicherheitserwägungen (38 %). OSS erleichtert zudem naturgemäß den Einsatz verschiedenartiger Lösungen auf verschiedenen Netzsegmenten oder Systemebenen (Multi-Vendor-Strategie), vor allem im Bereich der Server-Betriebssysteme. Die Umsetzung im Teilnehmerfeld zeigt Tabelle 5.

Content Security

Die größte bewusst aus Sicherheitsgründen eingesetzte Heterogenität findet man jedoch bei der Malware-Abwehr: Nur 41 % vertrauen hier noch auf einen einzigen Anbieter (vgl. Tab. 5), was in etwa dem Wert von 2004 entspricht. Der Anteil derjenigen, die sogar auf *drei* oder mehr unterschiedliche Lösungen setzen, hat sich jedoch im Vergleich zur vorigen Studie noch um vier Prozentpunkte erhöht.

Generell ist eine umfassende Lösung gefragt: Jeweils deutlich über 80 % erwarten von einer Content-Security-Solution außer der Abwehr von Viren auch Schutz vor Spyware und Spam. Monitoring und Alerting fordern etwa drei Viertel und jeweils knapp zwei Drittel wollen auch gleichzeitig Phishing-Abwehr, Inhaltsfilter und Reporting-Tools darin vorfinden.

Außer bei mobilen Systemen haben die Befragten die Update-Frequenz für Malware-Signaturen deutlich erhöht: Die mittleren Werte (Tab. 6) sind auf zentralen Systemen, PCs und Workstations heuer um jeweils rund sechs Stunden kürzer als vor zwei Jahren. Meistgenannt bleibt ein tägliches Update – bei den zentralen Systemen (Gateway und Server) gibt es aber mittlerweile genauso viele Teilnehmer, die ein stündliches Update vorsehen. Nochmals deutlich gestiegen ist zudem die Verbreitung von Online-Virenwächtern: Über zwei Drittel haben jetzt einen solchen Schutz auf den PCs ihres Hauses eingerichtet (2004: 52 %). Eine isolierte Test-Umgebung für Malware steht 48 % zur Verfügung.

Device-Management

Der erheblichen Gefährdung durch Plug&Play-(P&P)-Peripherie steht offenbar nur selten eine erwünschte Nutzung gegenüber: Auf die Frage nach der Bedeutung für die Wertschöpfungskette ihres Hauses antworteten die weitaus meisten Befragten, diese sei gering (37 %) oder vernachlässigbar (32 %) – 5 % sehen darin überhaupt keinen Nutzen, bei 10 % ist die Nutzung generell untersagt. Nur eine eher kleine Gruppe von Unternehmen und Behörden (15 %) gab eine „große" Bedeutung an. Eine Intensivierung des P&P-Einsatzes planen 25 %. Zur Sicherung der Schnittstellen gegen unerwünschte Aufschaltung von P&P-Devices dienen vor allem organisatorische Mittel (Verbot, Dienstanweisung usw.) – nur ein starkes Viertel nutzt „mitgelieferte" Sicherungsfunktionen der BIOS- oder Betriebssystem-(OS)Anbieter, noch weniger eine spezielle Schutzsoftware (s. Abb. 4).

Security-Management

Die Einschätzung der Wichtigkeit verschiedener Komponenten im Security-Management entspricht

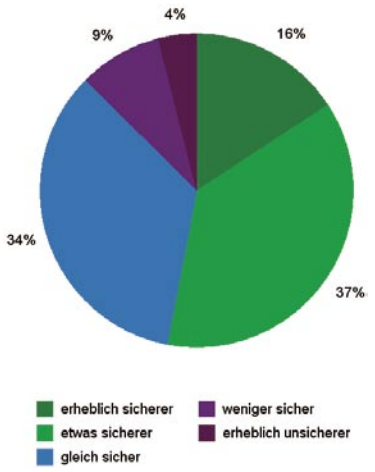

Abbildung 3: Einschätzung der Sicherheit von Open-Source-Software

Basis: 151 Antworten

Maßnahme	ja
Bordmittel des Betriebssystems	72%
Image-Restore mit „ausgespartem" Datenbereich	54%
Rettungs-/Live-CD des Betriebssystemanbieters	50%
Image-Restore unter Inkaufnahme eines evtl. Datenverlusts	46%
selbst erstellte Rettungs-/Live-CD	34%
frei erhältliche Unix-/Linux-Rettungs-/Live-CD	22%
Rettungs-/Live-CD eines kommerziellen Drittanbieters	20%
Sonstiges	6%
nichts dergleichen	1%

Basis: 158 Antworten

Tabelle 8: Vorgesehene Maßnahmen zum System-Recovery

Folgende Komponenten sind...	sehr wichtig	wichtig	unwichtig	Vergleichszahl
zentrale Überwachung der eingesetzten Security-Systeme	64%	32%	3%	1,61
plattformübergreifende Benutzerverwaltung	59%	37%	4%	1,54
Virtual Private Networks (VPN)	47%	46%	7%	1,4
Alarm- und Eskalationssystem	42%	52%	6%	1,35
Intrusion Detection Systems (IDS)	27%	55%	18%	1,09
Single-Sign-on	26%	50%	23%	1,03
Public Key Infrastructure (PKI)	24%	56%	20%	1,03
Kontrolle und Überwachung von Internet-Missbrauch	21%	57%	22%	0,99

Basis: Ø 153 Antworten

Tabelle 7: Security-Management

	ja	teilweise	nein
Aktionspläne für den K-Fall	50%	33%	17%
Recovery Units mit			
... Aktionsplan	39%	38%	23%
... Benötigte Ressourcen (HW,SW, etc.)	40%	31%	29%
Aktionspläne Störungen im Tagesbetrieb	41%	33%	26%
IT-Dokumentation (Arbeitsanweisungen)	52%	37%	12%
Allgemeine Dokumentationen	50%	39%	11%
Inventarisierung			
... Hardware	55%	30%	15%
... Software	52%	32%	16%
... Infrastruktur (Klima, etc.)	42%	31%	27%

Basis: Ø 124 Antworten

Tabelle 9: Umfang der Notfalldokumentation

in etwa den Angaben der vorigen Studie. An erster Stelle stehen eine zentrale Überwachung eingesetzter Sicherheitssysteme und eine plattformübergreifende Benutzerverwaltung (s. Tab. 7). Häufiger als 2004 wurde hingegen der Einsatz von Management-Lösungen zur System-Administration bejaht: 64 % nutzen für Netzwerksysteme Management-Lösungen der jeweiligen Hersteller (+14 Prozentpunkte), bei Host-/PC-Systemen sind es 55 % (+16). Mit zentralen Management-Lösungen arbeiten 44 % im Netzwerk (+8) beziehungsweise 50 % auf Hosts und PCs (+9). Dennoch verwalten aber heute 77 % der Befragten ihre Netzwerksysteme (auch) in nennenswertem Umfang manuell, bei Host-/PC-Systemen sind es 74 % (2004: 69 %/72 %). Ein Mehr an Management-Lösungen scheint also wider Erwarten keine Entlastung bei der „Handarbeit" zu bedeuten.

Die meistgeprüften Log-Files sind weiterhin jene von Anti-Malware-Lösungen, gefolgt von Firewall- und Intrusion-Detection-Protokollen – Meldungen von Netzkomponenten, Betriebssystemen und Applikationen werden hingegen überwiegend nur bei Bedarf ausgewertet (Details s. Abb. 5).

Für den „Fall der Fälle", dass ein System nicht mehr wie vorgesehen startet oder arbeitet, verlassen sich die meisten Studienteilnehmer zum System-Recovery auf die Mechanismen der Betriebssystemhersteller oder auf das Wiedereinspielen von Images – mit 46 % auch ein hoher Anteil unter Inkaufnahme eines eventuellen Datenverlusts seit der letzten Sicherung (Details s. Tab. 8).

Notfallvorsorge

Bei der räumlichen Trennung wesentlicher Komponenten der Informationsverarbeitung überwiegt erneut die Unterbringung in einem anderen Gebäude eine Separation durch Brandabschnitte. Vor allem Auslagerungsarchive (37 %) und

Die Auswertung der <kes>/Microsoft-Sicherheitsstudie erfolgte inklusive Erstellung der Ergebnistabellen und aller Grafiken größtenteils mit dem interaktiven Analysewerkzeug InfoZoom. Wir bedanken uns bei humanIT (www.humanit.de) für die freundliche Unterstützung in technisch-organisatorischer Hinsicht.

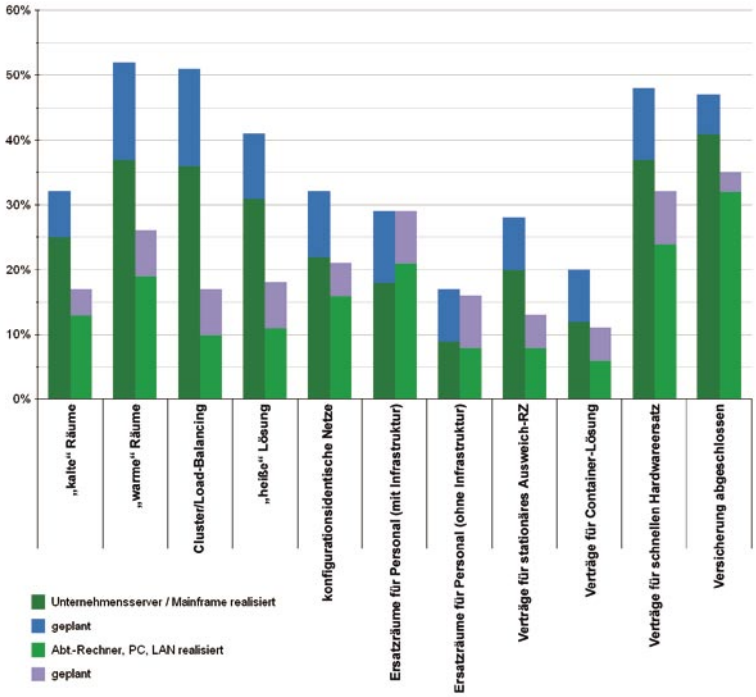

Abbildung 6: Bereitstellungen für längere Ausfälle bei IT-Systemen

Basis: Ø 120 Antworten

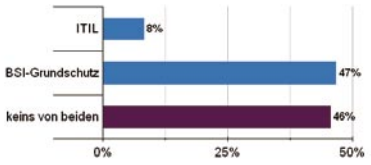

Abbildung 7: Berücksichtigung von Rahmenwerken bei Notfalldokumentationen

Basis: 90 Antworten

gespiegelte Daten (35 %), aber auch zusätzliche Rechner/Cluster (31 %) werden auf verschiedene Gebäude verteilt – andere Brandabschnitte genügen 26 % (Archive), 21 % (Mirror) beziehungsweise 18 %. Weiterhin eher selten ist die Auslagerung zu Partnern oder kommerziellen Anbietern (14 % / 8 % / 8 %). Für Robotersysteme überwiegt hingegen mit 58 % die Zahl der Befragten, die *keine* räumliche Trennung vorsehen.

Vergleicht man die Bereitstellungen beziehungsweise Planungen für längere Ausfälle (Abb. 6) mit den Angaben von 2004, so zeigt sich für Unternehmens-Server und Mainframes – neben einer höheren Vorsorgequote „in der Breite" – vor allem ein klarer relativer Bedeutungszuwachs so genannter „warmer" Lösungen, also von Räumen mit bereitstehender (wichtiger) Hardware. Lagen diese vor zwei Jahren noch mit „heißen" Backup-Systemen auf einem geteilten vierten Platz, so stehen sie jetzt unter Berücksichtigung geplanter Vorhaben an erster Stelle (52 %). Auch bei den realisierten Bereitstellungen (37 %) haben sie mit den Verträgen zur schnellen Ersatzlieferung gleichgezogen und landen hinter abgeschlossenen Versicherungen (41 %) auf Platz Zwei. „Kalte" Räume haben hingegen an Gewicht verloren.

Dass Recovery-Verträge auch tatsächlich genutzt werden mussten, berichteten diesmal gleich acht Studien-Teilnehmer, die Hälfte von ihnen erlebte sogar mehrere Ernstfälle; 46 Teilnehmer gaben hingegen an, einen bestehenden Recovery-Vertrag bislang noch nicht in Anspruch genommen zu haben.

Auch heuer bleiben „manuelle" Systeme bei der Notfall-Dokumentation führend: 64 % der Befragten haben ein solches „Handbuch" für den Notfall in (elektronischer) Textform vorliegen, weitere 19 % planen das; online-gestützte Dokumentationen findet man bei 31 % (20 % in Planung), ausgewachsene Online-Anwendungen nur bei 13 % (16 % i. P.). Die Aktualisierung von Notfall-Dokumentationen erfolgt weiterhin vorrangig anlassbezogen (82 %) – nur 11 % gaben an, dies regelmäßig zu tun (im Mittel etwa halbjährlich), 7 % erneuern ihre Pläne/Vorbereitung nie. Knapp die Hälfte der vorliegenden Dokumentationen deckt die Anforderungen des IT-Grundschutz' ab (s. Abb. 7). Zu den Inhalten der Notfall-Dokumentation siehe Tabelle 9.