

Inhaltsverzeichnis

Vorwort	9
----------------	----------

1. Datensicherung und Datensicherheit

1.1. So retten Sie die Dateien vom USB-Stick Ihres Mitarbeiters	10
1.2. So vermeiden Sie Datenverluste beim RAID-Recovery	12
1.3. Vermeiden Sie Datenverlust durch drei essentielle Maßnahmen	15
1.3.1 Technische Maßnahme: Wie Sie zentrale Datenspeicher erzwingen	15
1.3.2 Organisatorische Maßnahme: Regeln Sie die Verwendung des Datenspeichers per Policy	16
1.3.3 Persönliche Ebene: Klären Sie Ihre Anwender über den Sinn aller Maßnahmen auf	16
1.3.4 Fazit: Weitere Gefahren im Umgang mit Dateien ebenso akut	17
1.4. Wie Sie feststellen, ob alle Daten korrekt archiviert wurden	18
1.5. So beobachten Sie unbemerkte Zugriffe auf Ports	19
1.5.1 So betreiben Sie Ihren eigenen Mini-Honey-Port	19
1.5.2 Fazit: HoneyPorts bieten keinen proaktiven Schutz	20
1.6. Wie Sie sich vor Name-Server-Fälschungen sicher schützen – trotz geringer DNSSEC-Unterstützung	21
1.6.1 DNS-Angriffe: Wie Angreifer fremde und eigene Name-Server manipulieren	21
1.6.2 3 Schutzmaßnahmen: Wie Sie sich vor der Manipulationsgefahr schützen	21
1.6.3 So richten Sie DNSSEC praktisch ein	23
1.7. Mit diesen Maßnahmen schützen Sie Ihre Web-Browser vor Infektionen per DNS-Rebinding	24
1.7.1 DNS-Rebinding: Wie Angreifer die „Same Origin Policy“ im Browser durchbrechen	24
1.7.2 DNS Pinning: Warum die integrierte Schutzmaßnahme kein Universalschutz ist	25
1.7.3 Schutzmaßnahmen auf Netzwerkebene: Schaffen Sie eine sichere DNS-Infrastruktur	26
1.7.4 Alternative Schutzmaßnahme für kleine Netzwerke: Nutzen Sie spezielle Host-Firewalls	26
1.7.5 Schutzmaßnahmen auf Host-Ebene: Härten Sie Ihre Browser-Plugins	26
1.7.6 Wie Sie 3 fiese Spionagelücken im Flash-Player endlich sicher beheben	27
1.7.7 Licht ins Dunkel: Wie Sie das Flash-Player-Plugin überhaupt konfigurieren können	27
1.7.8 So löschen Sie Cookies automatisch nach jeder Surf-Sitzung	29
1.7.9 Netzwerkeinstellungen: Geben Sie alle Einstellungen zentral in Ihrem Netzwerk vor	30
1.7.10 Ausblick: Steuern Sie die Sicherheit von lokalen Flash-Anwendungen	30
1.7.11 Fazit: Eine reale Gefahr mit viel Potenzial	30

1.8. VPN-Killer von Microsoft? Wie Sie mit DirectAccess sichere Remote-Zugänge einrichten	32
1.8.1 Warum durch die Nutzung von IPv6 der Planungs- und Konfigurationsaufwand steigt	32
1.8.2 Wann Sie trotz erhöhtem Konfigurationsaufwand von DirectAccess profitieren	33
1.8.3 So meistern Sie die knifflige Server- und Client-Installation von DirectAccess	34
1.8.3.1 Architektur: Entscheiden Sie sich für die richtigen Protokolle	34
1.8.3.2 Vorbereitung: Diese Komponenten müssen bereits im Netzwerk laufen	35
1.8.3.3 Server-Implementierung: Konfigurieren Sie Ihren Server mit diesem Assistenten	35
1.8.3.4 Client-Implementierung: Wie Sie Ihre Clients mit dem DirectAccess-Server verbinden	37
1.8.4 Fazit: Die Geduld zahlt sich aus	37
1.9. Wie Sie sensible Notizen und Binärdaten in chiffrierten Containern speichern	38
1.9.1. So erzeugen Sie Ihren chiffrierten Textdateien-Container	38
1.9.2 So fügen Sie weitere Benutzerkennwörter hinzu	39
1.10. Schützen Sie sich vor gefährlichen XSS-Angriffen	40
1.10.1 Kenne deinen Feind: Wie XSS-Angriffe funktionieren	40
1.10.2 Warum Ihre Mitarbeiter besonders gefährdet sind	40
1.10.3 So schützen Sie Ihre Anwender vor XSS-Attacken	41
1.10.4 Ausblick: Wie Sie Ihre eigenen Web-Anwendungen vor XSS-Angriffen schützen	42
1.11. So schützen Sie Ihre Unternehmens-Website vor XSS-Angriffen	43
1.11.1 Das müssen Sie für einen wirksamen Anti-XSS-Schutz beachten	43
1.11.2 Universaler XSS-Schutz: Schützen Sie Ihre Web-Anwendungen durch eine Web-Application-Firewall	43
1.11.3 Wie Sie Ihre Web-Anwendungen per Web Application Firewall abdichten	44
1.11.4 Wann Sie eine Web Application Firewall am besten einsetzen	44
1.11.5 Fremdentwickelte Systeme: Sorgen Sie für regelmäßige Updates und Sicherheits-Scans	45
1.11.6 Eigenentwickelte Systeme: Wie Sie die komplizierte Selbstabsicherung meistern	45
1.11.6.1 XSS-Sicherheitslücken aufdecken: Machen Sie aus Sicht eines Angreifers die XSS-Schwachstellen ausfindig	45
1.11.6.2 XSS-Sicherheitslücken schließen	46
1.11.7 Fazit: Ein wirksamer Schutz erfordert Ihre Disziplin	47
1.12. Wie Sie Ihre Benutzer vor bösartiger Webcam- und Mikrofon-Spionage schützen	48
1.12.1 Warum diese Spionageangriffe auf Ihr Unternehmen eine ernste Gefahr sind	48
1.12.2 Wie Sie sich vor der digitalen Wanze schützen	48
1.12.3 Fazit: Auf die Mischung kommt es an	50
1.13. Wie Sie mit Token-basierter Zentralchiffrierung Ihre Notebooks vor Datendiebstahl schützen	51

1.13.1 Wie Sie die Daten auf Ihren Notebooks per USB-Token unknackbar chiffrieren	51
1.13.1.1 TrueCrypt: Kostenlose Vollverschlüsselung	52
1.13.1.2 So erstellen Sie Ihren verschlüsselten Container	52
1.13.1.3 Wie Sie auf die verschlüsselten Daten komfortabel per USB-Token zugreifen	54
1.13.2 Auswahl: Diese Kriterien müssen Sie bei der Auswahl Ihrer Lösung beachten	54
1.13.3 Implementieren: Wie Sie die Lösung im Netzwerk einführen	55
1.13.4 Fazit: Geduld ist gefragt	57

2. Virenschutz, Malware

2.1. Wie Sie Malware-Prozesse zweifelsfrei identifizieren	58
2.1.1 Eigenschaftsbasierte Erkennung: So decken Sie auch versteckte Prozesse auf	58
2.1.2 Wie Sie in der Processlibrary Ihren Verdacht erhärten	58
2.2. So verhindern Sie die ungewollte Datenweitergabe durch Office-Meta-Daten	60
2.2.1 Wie Sie SendShield konfigurieren	60
2.2.2 Wie SendShield Ihre Anwender unterstützt	61
2.2.3 Fazit: Sicherheit hat ihren Preis	61
2.3. Wie uns Cloud-basierte Malware-Scanner vor neuen Viren schützen sollen und welche Risiken entstehen	62
2.3.1 Prinzip: Was Malware-Scanner in der Cloud tatsächlich leisten	62
2.3.2 Anbieter: Diese Cloud-Lösungen existieren	63
2.3.3 Chancen und Risiken: Verzichten Sie zunächst auf den Einsatz!	63
2.4. Wann Microsofts kostenloser Virenschutz Ihre Systeme tatsächlich sicher schützt	65
2.4.1 Schutz im Vergleich: Das leistet Microsoft Security Essentials tatsächlich	65
2.4.2 So konfigurieren Sie Microsoft Security Essentials in der Praxis	66
2.5. Identifizieren und beseitigen Sie Spionageprogramme mit dem neuen a-squared HijackFree	68
2.5.1 Wie Sie Prozesse und Verbindungen analysieren	68
2.5.2 Decken Sie hemmungslos alle Internet-Explorer-Addons auf	68
2.5.3 Handeln statt beobachten: So entfernen Sie lästige Programme	69

3 Troubleshooting und Werkzeuge für den Administrator

3.1. Wie Sie Ihren Support dank bebildelter Problembeschreibungen entlasten	70
3.1.1 Das zeichnet der neue Problem Steps Recorder für Sie auf	70

3.1.2	So setzen Ihre Mitarbeiter den Problem Steps Recorder ein	70
3.1.3	So wertet Ihr Support den Bericht aus	71
3.2.	Versteckte Arbeitsspeicherprobleme aufdecken	72
3.2.1	Symptome: Wie sich Arbeitsspeicherfehler in der Praxis äußern	72
3.2.2	Ursachen: Warum RAM-Defekte auftreten	72
3.2.3	Analyse: Wie Sie den Defekt systematisch aufdecken	73
3.2.4	Lösung: Tauschen Sie das Speichermodul aus	75
3.2.5	Vorbeugung: Wie Sie RAM-Defekten vorbeugen	75
3.3.	Nutzen Sie Ihren individuellen Security-Werkzeugkoffer auf USB-Stick	77
3.3.1	Wie Sie PortableApps auf Ihrem Admin-Stick installieren	77
3.3.2	So stellen Sie Ihren persönlich Security-Werkzeugkoffer zusammen	78
3.4.	Wie Sie Festplattenprobleme gezielt diagnostizieren	79
3.5.	Wie Sie mit IPMI und Nagios Ihre Server-Hardware überwachen und drohende Ausfälle frühzeitig erkennen	81
3.5.1	Nagios-Monitoring: Mit diesem Modul überwachen Sie IPMI	81
3.5.2	Konfigurationsübersicht: Unterscheiden Sie diese vier Konfigurationsdomänen	81
3.5.4	Ausblick	82
3.6.	Mit ELog dokumentieren Sie lückenlos alle Änderungen an Ihrer Netzwerkinfrastruktur	83
3.6.1	So schnell steht Ihnen ELog zur Verfügung	83
3.6.2	Wie Sie ELog für die Protokollierung nutzen	84
3.7.	Finden Sie ressourcenhungrige Prozesse und vermeiden Sie Systemabstürze mit dem Usage Monitor	85
3.7.1	So konfigurieren Sie Ihre Überwachungs-Limits	85
3.7.2	Legen Sie automatische Reaktionen beim Erreichen von Schwellenwerten fest	85
3.8.	So decken Sie Fehlkonfigurationen mit dem IT Environment Health Scanner auf	87
3.9.	Die 6 besten Dateibeobachtungs-Tools für Windows XP und Vista	89
3.9.1	Decken Sie alle geöffneten Dateien auf	89
3.9.2	Beobachten Sie die Dateizugriffe live	89
3.9.3	So protokollieren Sie Dateizugriffe	89
3.9.4	Wie Sie versteckte Daten-Streams finden	90
4.	System- und Netzwerküberwachung	
4.1.	Mit dem IDS Policy Manager verwalten Sie Ihr Intrusion-Detection-System	91

4.1.1	So konfigurieren Sie das Werkzeug für die Erstverwendung	91
4.1.2	So verteilen Sie die Policy an Ihre Sensoren	93
4.1.3	Fazit: Noch nie war die Snort-Administration so einfach	93
4.2.	So decken Sie veraltete Software-Versionen auf Ihren Workstations auf	94
4.2.1	Einzelplätze prüfen: Mit diesen Tools nehmen Sie eine kostenlose Überprüfung vor	94
4.2.2	Netzwerke prüfen: So nehmen Sie massenweise Versionschecks für Ihre Anwendungen vor	94
4.3.	So entdecken Sie fremde Geräte in Ihrem Netzwerk	96
4.4.	So erhalten Sie alle wichtigen Analyseinformationen mit zwei Mausklicks	97
4.5.	Mit AccessChk decken Sie falsche Zugriffsrechte auf Ihrem Windows-File-Server blitzschnell auf	99
4.5.1	So nutzen Sie AccessChk für die Überprüfung Ihrer NTFS-Zugriffsrechte	99
4.5.2	Praxisbeispiel: Wie Sie zwei konkrete Sicherheitsüberprüfungen mit AccessChk realisieren	100
5.	Richtlinien	
5.1.	Wie Sie den Risikofaktor Mensch entschärfen	101
5.2.	Falle 1: Fremde Personen haben unkontrollierten Zugang zu Ihren Räumlichkeiten	102
5.3.	Falle 2: Unbefugte Personen nutzen Geräte	102
6.	Dokumentation	
6.1.	So verwenden Sie Steganos LockNote	105
6.2.	Speichern Sie Ihre Notizen in beliebig vielen Dateien	106
7.	Nützliche Links für Ihren Admin-Alltag	107
8.	Index	109