

Grundschutz und Sicherheit PC

Fragebogen Sicherheitsbedarf

Hier finden Sie:

Fragen zum Schutzbedürfnis Ihrer Daten
Seite 2

Fragen zur Sicherheit im Internet und e-Banking
Seite 6

Fragen zu Ihrem Konzept zur Datensicherheit
Seite 8

Über den Autor
Seite 10

Dr. Hansgeorg Schaller
<http://www.hg-schaller.de>
[post\(at\)hg-schaller.de](mailto:post(at)hg-schaller.de)

Bitte ersetzen sie (at) durch @!

Dieser Fragebogen wendet sich an Nutzer von PCs („Stand-Allone“ PCs), die als Einzelarbeitsplätze mit oder ohne Anschluss zum Internet fungieren. Das können Privatleute oder Selbstständige sein. Sinngemäß kann der Fragebogen auch als Richtlinie für kleine Unternehmen mit kleinen Netzwerken dienen.

Die nachfolgenden Fragen dienen dazu, den Schutzbedarf der auf Ihrem Computer gespeicherten Daten abzuschätzen. Unter Daten werden in diesem Zusammenhang alle digitalen, auf dem Computer gespeicherten Informationen, wie Bilder, Adressen, Dokumente und sonstigen Informationen, verstanden werden. Der Schutzbedarf richtet sich nach der Sensibilität der Daten, deren persönlicher Bedeutung für Sie und der Schwierigkeit der Wiederherstellung verlorener Daten. Zu Beachten sind drei Bereiche: 1. Schäden durch Diebstahl von Daten und deren Missbrauch durch Dritte, 2. Schäden dadurch, dass der Compu-

ter zeitweise nicht zur Verfügung steht und 3. Schäden durch irreversiblen Datenverlust.

Bitte beantworten Sie die nachfolgenden Fragen vollständig und ehrlich nach bestem Wissen und Gewissen. Im Zweifel bewerten Sie die Gefahr/den Schaden lieber höher als zu niedrig.

Dieser Fragebogen ist dazu gedacht, Sie für die Risiken und Probleme bei der Nutzung Ihres Computers zu sensibilisieren und Sie zum Nachdenken über die Gestaltung von Sicherheitsmaßnahmen zu bringen.

Professionelle Anwender wenden sich sinnvollerweise an ein Beratungshaus Ihres Vertrauens. Weitere Informationen und Anregungen finden sich unter anderem auf den Seiten des Bundesamt für Sicherheit in der Informationstechnik (BSI):

<http://www.bsi.de>
Hier kann auch das komplette IT Grundschutzhandbuch kostenlos als Dokument im PDF Format herunter geladen werden: <http://www.bsi.de/gshb/deutsch/download/index.htm>

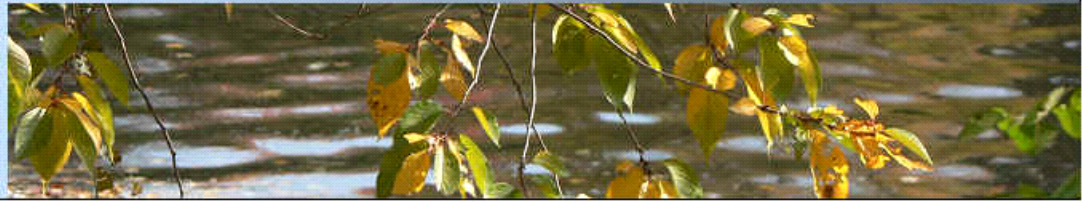
(ca.35 MB Daten, 3096 Seiten) - obigen Link bitte in einer Zeile aus-schreiben.

Haftungsausschluss

Der Autor übernimmt keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der bereitgestellten Informationen. Haftungsansprüche gegen den Autor, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, sofern seitens des Autors kein nachweislich vorsätzliches oder grob fahrlässiges Verschulden vorliegt.

Copyright

Eine Vervielfältigung oder Verwendung dieses Textes in anderen elektronischen oder gedruckten Publikationen ist ohne ausdrückliche Zustimmung des Autors nicht gestattet.



Die nachfolgend gemachten Angaben beziehen sich auf folgendes Computer-System (Stand-Allone PC):

Name Anwender: _____

Bezeichnung System: _____

Inventarnummer: _____

Seriennummer Prozessor: _____

Status / Datum: _____

Angaben zur Software und zum Betriebssystem siehe Seite 4 folgend.

Hier finden Sie:

Fragen zum Schutzbedürfnis Ihrer Daten Seite 2

Fragen zur Sicherheit im Internet und e-Banking Seite 6

Fragen zu Ihrem Konzept zur Datensicherheit Seite 8

Über den Autor Seite 10

Gefahr des Datendiebstahls und Missbrauchs durch Dritte:

Sind auf dem Rechner Daten gespeichert, die aufgrund gesetzlicher Vorschriften des Datenschutzes besonders geschützt werden müssen?

Beispiele: Namen und/oder Daten von Patienten, Kunden und Geschäftspartnern

ja	Nein	Weiß nicht
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Sind auf dem Rechner Daten gespeichert, bei denen Sie sich verpflichtet haben, diese besonders zu schützen?

Beispiele: Namen und/oder Daten von Vereinsmitgliedern, Freunden, Partnern etc.

ja	Nein	Weiß nicht
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Sind auf dem Rechner Daten gespeichert, die wenn Sie Dritten zugänglich werden würden, dazu genutzt werden könnten um in Ihrem Namen Geschäfte zu tätigen, um Ihnen zu schaden oder Sie zu erpressen?

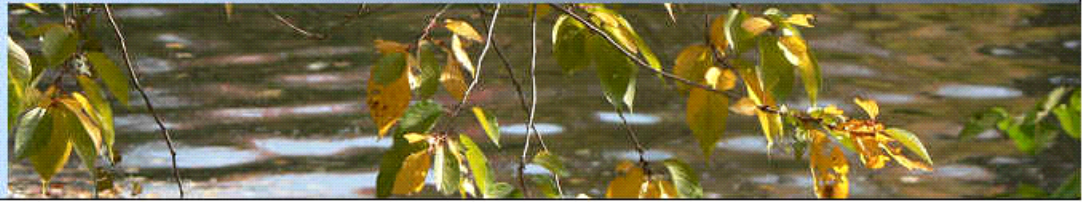
Beispiele: pornographische Darstellungen, Bewerbungsunterlagen, Namen von Bekannten, ihnen anvertraute Unterlagen Dritter, Daten oder Details zu Konten und oder Vermögenswerten (insbesondere Electronic Banking), Daten der Steuererklärung, geschäftliche Daten (Kalkulationen, Umsätze, Preise, Leistungsbeschreibungen, Angebote und sonstige Informationen)

ja	Nein	Weiß nicht
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Sind auf dem Rechner Zugangsdaten, PIN-Nummern oder Cookies gespeichert, die Sie benutzen, um sich über ihren Computern bei Dritten, wie z.B. Internet Providern, Yahoo oder anderen Diensten, anzumelden?

ja	Nein	Weiß nicht
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Dr. Hansgeorg Schaller
<http://www.hg-schaller.de>
[post\(at\)hg-schaller.de](mailto:post(at)hg-schaller.de)
 Bitte ersetzen sie (at) durch @!



Schäden die dadurch entstehen, dass Ihnen Ihr Computers nicht zur Verfügung steht:

Wie lange können Sie ihre persönlichen und geschäftlichen Aktivitäten in einem für Sie akzeptablen Maß aufrechterhalten, ohne dass Ihnen dafür Ihr Computer (bzw. Teil-Systeme Ihres Computers) zur Verfügung steht?

Hier finden Sie:

Fragen zum Schutzbedürfnis Ihrer Daten Seite 2

Fragen zur Sicherheit im Internet und e-Banking Seite 6

Fragen zu Ihrem Konzept zur Datensicherheit Seite 8

Über den Autor Seite 10

	Einige Stunden	Einen Tag	Ein Wochenende	Eine Woche	Unwichtig
E-Mail (Kommunikation: Anfragen stellen und beantworten, Dokumente verschicken)					
Internet (Recherche, Kaufen und Verkaufen)					
Briefe schreiben					
Bankgeschäfte erledigen					
Adressen und Telefonnummern herausfinden					
Reisen planen					
Drucke erstellen von Dokumente, Broschüren, Informationen oder andere Angelegenheiten					
Sonstige private Aktivitäten (wie Spiele, Nachrichten hören, sich Informiert halten, Weiterbildung, Verein verwalten)					
Sonstige geschäftliche Aktivitäten (wie Reisekosten abrechnen, Buchhaltung, Präsentationen, Kundenanfragen bearbeiten, Planen und so weiter)					

Welche Anwendungen (wie z..B. Schreibprogramm, Buchhaltungssoftware, Internet etc.) benötigen Sie unbedingt und können (wollen) nicht darauf verzichten:

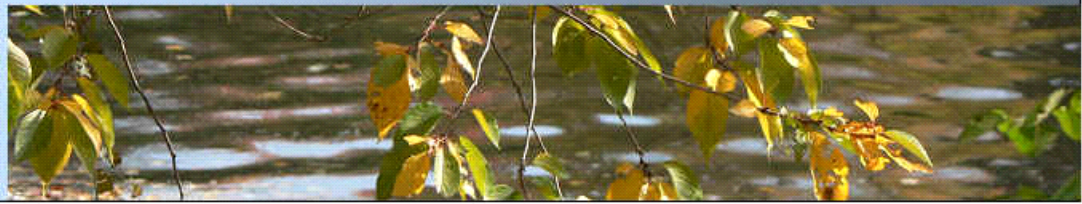
.....

.....

.....

Dr. Hansgeorg Schaller
<http://www.hg-schaller.de>
[post\(at\)hg-schaller.de](mailto:post(at)hg-schaller.de)

Bitte ersetzen sie (at) durch @!



Schaden durch Datenverlust

Die nachfolgenden Fragen dienen dazu, zu beurteilen, ob und mit welchem Aufwand Sie die Funktionsfähigkeit ihres Computers und die darauf gespei-

Hier finden Sie:

Fragen zum Schutzbedürfnis Ihrer Daten Seite 2

Fragen zur Sicherheit im Interne und e-Banking Seite 6

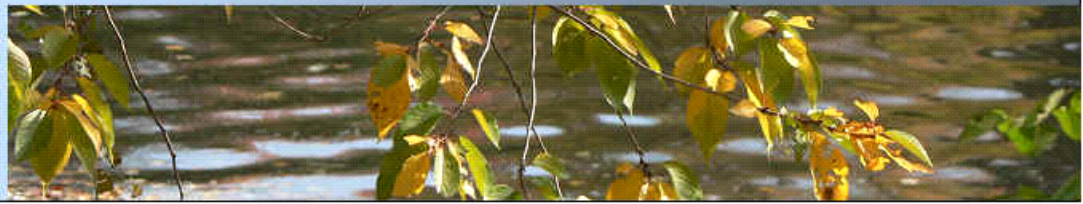
Fragen zu Ihrem Konzept zur Datensicherheit Seite 8

Über den Autor Seite 10

Dr. Hansgeorg Schaller
<http://www.hg-schaller.de>
[post\(at\)hg-schaller.de](mailto:post(at)hg-schaller.de)

Bitte ersetzen sie (at) durch @!

Frage	Welches Betriebssystem verwenden Sie? Bitte geben Sie die aktuelle Version exakt an! Beispiel: MS Windows XP, Professional Edition, Service Pack 2	Haben Sie für dieses Betriebssystem die original Datenträger (CD-ROM, Disketten etc.), von denen Sie aus das Betriebssystem erneut installieren können?	Können Sie ein vom Original Datenträger erneut installiertes Betriebssystem bei Bedarf updaten?	Haben Sie zu dem Betriebssystem die dazugehörigen Aktivierungs-Codes bzw. Installations-Passwörter/Codes im Original bzw. können Sie das Betriebssystem gegebenenfalls bei Microsoft freischalten?
B		Ja / nein	Ja / nein	Ja / nein
Frage	Welche Software (Anwendungsprogramme) verwenden Sie? Nennen Sie das Programm und seine exakte Version! Also zum Beispiel: MS Word 2003 (SP2) oder Adobe Acrobat Writer 5.0 Die genaue Information finden Sie normalerweise unter dem Knopf „?“.	Haben Sie für diese Software die original Datenträger (CD-ROM, Disketten etc.), von denen Sie aus die Software erneut installieren können?	Können Sie eine vom Original Datenträger erneut installierte Software nach einer erneuten Installation updaten?	Haben Sie zu der Software die dazugehörigen Aktivierungs-Codes bzw. Lizenzcodes im Original?
1		Ja / nein	Ja / nein	Ja / nein
2		Ja / nein	Ja / nein	Ja / nein
3		Ja / nein	Ja / nein	Ja / nein
4		Ja / nein	Ja / nein	Ja / nein
5		Ja / nein	Ja / nein	Ja / nein
6		Ja / nein	Ja / nein	Ja / nein
7		Ja / nein	Ja / nein	Ja / nein
8		Ja / nein	Ja / nein	Ja / nein
9		Ja / nein	Ja / nein	Ja / nein



Fragenkatalog zur Sicherheit

Die nachfolgenden Fragen dienen dazu, abzuschätzen, ob die von Ihnen getroffenen Sicherheitsmaßnahmen ausreichend sind, um Ihrem Schutzbedarf gerecht zu werden. Wie groß der Schutzbedarf ist, sollte sich aus der Beantwortung der auf den vorherigen Seiten aufgeführten Fragen ergeben haben.

Wenn Sie sensible Daten (Missbrauch) auf Ihrem Rechner gespeichert haben:

- Haben Sie Ihr Computer gegen Diebstahl geschützt? Haben Sie Ihren Computer gegen die Nutzung durch einen unbefugten Dritten geschützt? Würde Ihnen ein Diebstahl sofort auffallen?
- Ist der Zugang zu Ihrem Rechner mit einem Passwort geschützt?
- Müssen Sie ein Passwort eingeben, wenn Sie den Rechner aus dem Modus des Bildschirm-Schoners wieder aktivieren wollen?
- Sind ihre sensiblen Daten verschlüsselt?
- Ist Ihre gesamte Festplatte verschlüsselt?
- Sind die Daten in allen Sicherheitskopien verschlüsselt?
- Sind die Datenträger, die Sie für die Sicherheitskopien verwenden, physikalisch gegen Diebstahl geschützt?

Sicher sind Ihre Daten nur dann, wenn sie alle diese Fragen mit „ja“ beantworten können.

Wenn Sie Passwörter oder Zugangcodes verwenden

- Welche Vorkehrungen haben Sie für den Fall getroffen, dass Sie Ihr Passwort vergessen?
- Haben Sie Ihr(e) Passwort(e) aufgeschrieben/notiert?
- Sind Ihr(e) Passwort(e) Dritten bekannt?
- Kann ein Dritter diese Notiz(en) (leicht?) auffinden?

Wenn Sie wichtige und sensible Daten gespeichert und abgesichert haben, so könnte der Fall eintreten, dass Sie handlungsunfähig werden, und ein Dritter auf Ihre gespeicherten Unterlagen zugreifen muss. Wenn dieses relevant ist:

- Welche Vorkehrungen haben Sie für diesen Fall getroffen?

Wenn Sie ihren Computer nicht an das Internet oder ein internes Netzwerk (Intranet) angeschlossen haben, so können Sie die folgenden Fragen übergehen. Ansonsten sollten Sie folgende Fragen beantworten:

- Verwenden Sie eine „Firewall“?
- Welche „Firewall“ verwenden Sie? Name/Bezeichnung:.....
- ist die „Firewall“ aktuell, aktualisieren Sie sie regelmäßig?
- Verwenden Sie eine Virenschutz Software?
- Welchen Virenschutz verwenden Sie? Name/Bezeichnung:.....
- Ist die Virenschutzsoftware aktuell, aktualisieren Sie sie regelmäßig?
- Sind die Virendefinitionen aktuell, aktualisieren Sie die Definitionen täglich?
- Verwenden Sie eine Software zum Schutz gegen „Spyware“ und Trojaner?
- Wenn ja, welche Software verwenden Sie?
- Ist diese Software aktuell, aktualisieren Sie sie regelmäßig?
- Aktualisieren Sie Ihr Betriebssystem, Ihren Internetbrowser und Ihre Anwendungsprogramme regelmäßig?

Hier finden Sie:

Fragen zum Schutzbedarfnis Ihrer Daten
Seite 2

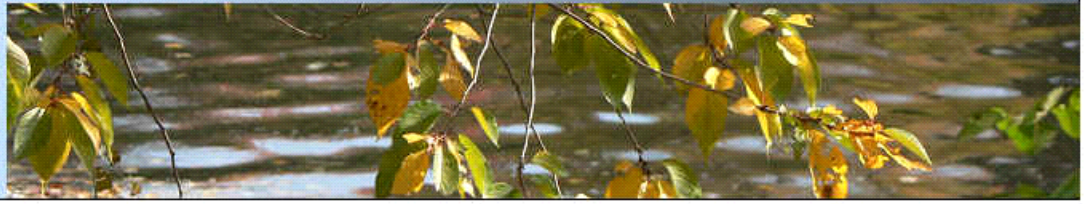
Fragen zur Sicherheit im Interne und e-Banking
Seite 6

Fragen zu Ihrem Konzept zur Datensicherheit
Seite 8

Über den Autor
Seite 10

Dr. Hansgeorg Schaller
<http://www.hg-schaller.de>
[post\(at\)hg-schaller.de](mailto:post(at)hg-schaller.de)

Bitte ersetzen sie (at) durch @!



Hier finden Sie:

**Fragen zum
Schutzbedürfnis
Ihrer Daten
Seite 2**

**Fragen zur
Sicherheit im
Interne und e-
Banking
Seite 6**

**Fragen zu Ihrem
Konzept zur
Datensicherheit
Seite 8**

**Über den Autor
Seite 10**

**Dr. Hansgeorg Schaller
<http://www.hg-schaller.de>
[post\(at\)hg-schaller.de](mailto:post(at)hg-schaller.de)**

Bitte ersetzen sie (at) durch @!

- Sind die Einstellungen ihres Internet-Browser und Ihrer Firewall auf hohe Sicherheit eingestellt (ActiveX und JavaScript deaktiviert; Sicherheit „Hoch“, und nutzen sie die „Vertrauenswürdigen Sites“ nur restriktiv)?
- Sind Sie sich über die Gefahren und Risiken bewusst, die Sie eingehen, wenn Sie persönliche Daten (Namen, Bankverbindung, Kreditkartendetails etc.) auf Webseiten eingeben?
- Sind Sie sich der Gefahren von „Pishing-Mails“ (antworten Sie auf per E-Mail an Sie gestellte Anfragen mit der Eingabe von Daten auf Webseiten) bewusst? Sicher sind sie nur, wenn sie alle diese Fragen mit „ja“ beantworten können.

Wenn Sie ihr Bankkonto on-line führen (E-Banking), so sind die folgenden spezifischen Fragen für Sie relevant.

- Machen Sie nur Abfragen zum Kontostand (= niedriges Risiko)?
- Führen Sie Transaktionen durch (= hohes Risiko)?

Welches Verfahren verwenden Sie, um Ihre Transaktionen durchzuführen?

- PIN/TAN Verfahren (über Webbrowser)
- PIN/e-TAN Verfahren (über Webbrowser)
- HBCI mit Diskette (mit speziellem Bank-Programm)
- HBCI mit Chipkarte (Chipkartenleser Sicherheitsklasse 1 und speziellem Bank-Programm)
- HBCI mit Chipkarte (Chipkartenleser Sicherheitsklasse 2 oder 3 und speziellem Bank-Programm)
- Verwahren Sie Ihre TAN Liste / HBCI Diskette / Ihre HBCI Chipkarte sicher und getrennt von andern Unterlagen auf?
- Haben Sie Ihre PIN-Nummer nur auswendig gelernt?

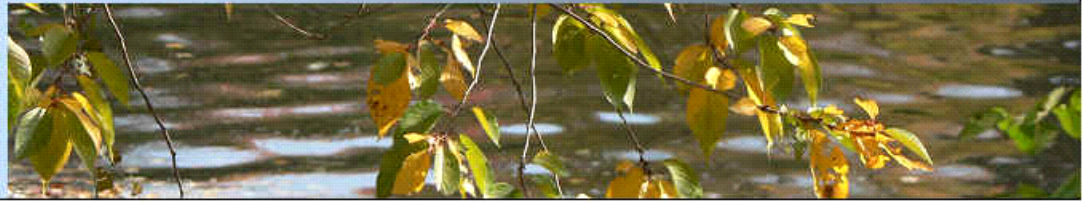
Ein spezielles Bank-Programm ist eine Anwendungssoftware wie z.B. StarMoney oder WisoMoney oder vergleichbare Software.

Die oben genannten Verfahren reichen von recht unsicher bis zu hoher Sicherheit (in der Reihenfolge ansteigender Sicherheit). Das HBCI-Verfahren mit ein Programm wie StarMoney in Verbindung mit einem Kartenleser Klasse 3, einer aktuellen Firewall und einer Virus-/Spywareschutz-Software ist (momentaner Stand) so gut wie absolut sicher - der verbleibende Schwachpunkt ist dann die Sicherheitskonzeption ihrer Bank.

Während sich die vorstehenden Fragen mit der Sicherheit ihrer Daten und Anwendungen durch Angriffe Dritter beschäftigten, so dienen die nachfolgenden Fragen dazu, die Sicherheit Ihrer Daten und Anwendungen gegen einen Datenverlust zu prüfen. Gefahren sind: Anwenderfehler, fehlerhafte Programme, elementare Schadensereignisse wie Wasser, Feuer, Magnetfelder, Strahlung (UV-Licht, Radiowellen) und mechanische Fehler (Materialfehler, Materialermüdung).

**Es gibt nur zwei Arten von Daten:
Gesicherte Daten und Daten, die noch nicht verloren gegangen sind.**

Das erforderliche Ausmaß der Datensicherung richtet sich nach dem Schutzbedürfnis der Daten. Die Verfahren zur Datensicherung sollten in einem Sicherheitskonzept schriftlich festgelegt und ihre Durchführung schriftlich dokumentiert werden.



Fragenkatalog zur Datensicherheit

Im Folgenden wird unter Datensicherung / Datensicherheit die Sicherung der Daten und Anwendungsprogramme, das so genannte Back-Up Konzept, also die Herstellung von Sicherheitskopien, verstanden.

Hier finden Sie:

Fragen zum Schutzbedürfnis Ihrer Daten
Seite 2

Fragen zur Sicherheit im Interne und e-Banking
Seite 6

Fragen zu Ihrem Konzept zur Datensicherheit
Seite 8

Über den Autor
Seite 10

- Haben Sie Erfahrungen damit (haben Sie es bereits einmal geübt), Ihr Computersystem mit Hilfe einer Datensicherung wieder herzustellen?

Wenn Sie keine Erfahrungen damit haben, Ihr Computersystem mit Hilfe einer Datensicherung wieder herzustellen:

- Haben Sie ausreichende Kenntnisse zur Datenwiederherstellung Ihres Systems?
- Haben Sie eine ausreichende Dokumentation zur Datenwiederherstellung Ihres Systems?
- Haben Sie ausreichende externe Ressourcen zur Datenwiederherstellung Ihres Systems (z.B. mittels eines PC-Wartungsvertrags)?

Wo verwahren Sie die Datenträger, mit deren Hilfe Sie Ihre Daten und Anwendungsprogramme wieder herstellen können (Sicherheitskopien)?

- In einem anderen Gebäude mit hoher Sicherheit (z.B. Bankschließfach)?
- In einem anderen Gebäude?
- Im gleichen Gebäude wie der eigentliche Computer, aber in einem anderen Raum (ggfls in einem Sicherheitsschrank)?
- Im gleichen Raum wie der eigentliche Computer und in einem Sicherheitsschrank?
- Im gleichen Raum wie der eigentliche Computer?
- In der Nähe/Griffweite des eigentlichen Computers?
- Direkt in dem eigentlichen Computer (separate Partition / zweite Festplatte)?
- Gar keine Sicherheitskopie?

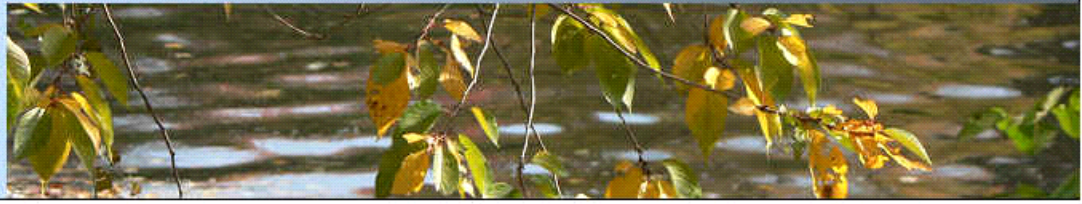
Die genannten Aufbewahrungsorte sind von oben nach unten in fallender Sicherheit, aber steigender Bequemlichkeit gelistet.

Wie häufig fertigen Sie Sicherheitskopien, die sie als „Langzeit-Sicherungskopie“ unter hoher Sicherheit aufheben?

- Vor jedem wichtigen Computer / Software Update?
- Regelmäßig, alle Tage / Wochen?
- Jedesmal, nachdem wichtige Daten auf dem Computer abgespeichert wurden?

Wie häufig fertigen Sie Sicherheitskopien, die sie als „Kurzzeit-Sicherungskopie“ unter niedriger Sicherheit aufheben?

- Vor jedem wichtigen Computer / Software Update?
- Regelmäßig, alle Tage / Wochen?
- Jedesmal, nachdem wichtige Daten auf dem Computer abgespeichert wurden?
- Welche Medien (CD-ROM, DVD, externe Festplatten) verwenden Sie für die Sicherheitskopien, und wie haben Sie sichergestellt, dass diese Medien auch über die beabsichtigte Lagerdauer hinaus lesbar sein werden?



- Wie überprüfen Sie, und wie häufig überprüfen Sie, dass diese Medien funktionieren (dass die Sicherheitskopien bei Bedarf wieder auf Ihren Computer eingespielt werden können)?

Zur Anfertigung von Sicherheitskopien gibt es verschiedene Ansätze: Komplettsicherung der Festplatte und Teilsicherung (relevanter Daten).

Hier finden Sie:

Fragen zum Schutzbedürfnis Ihrer Daten
Seite 2

Fragen zur Sicherheit im Internet und e-Banking
Seite 6

Fragen zu Ihrem Konzept zur Datensicherheit
Seite 8

Über den Autor
Seite 10

Sicherung als Image der Festplatte

Zur Komplettsicherung der Festplatte verwendet man entweder eine gespiegelte Festplatte, oder erzeugt man ein Image (ein Abbild) der Festplatte und speichert dieses in eine Archivdatei auf einer externen Festplatte oder DVDs

Vorteil: schnelle Wiederherstellung von Daten, Einstellungen und Anwendungsprogrammen

Nachteil: Kosten (spezielles Programm nötig), Dauer und Bedarf an Speicherplatz.

Daten können nicht ohne weiteres auf einen anderen Rechner transferiert werden.

Gefahr: ist das System mit Viren verseucht oder fehlerhaft konfiguriert, so werden diese Fehler mit in die Sicherheitskopie übernommen!

Sicherung der Anwender-Daten:

Relevante Daten (z.B. der Ordner „meine Dateien“ in MS Windows) werden (mittels Standard Programmen des Betriebssystems, wie z.B. dem MS Explorer) auf ein geeignetes Medium (Server, externe Festplatte, USB Stick) kopiert oder mit einem Brennerprogramm auf CD-ROM oder DVD gebrannt.

Vorteil: schnell, unkompliziert, billig, Daten können schnell wieder zurückgespielt werden, Daten können auf anderen Rechnern bearbeitet werden

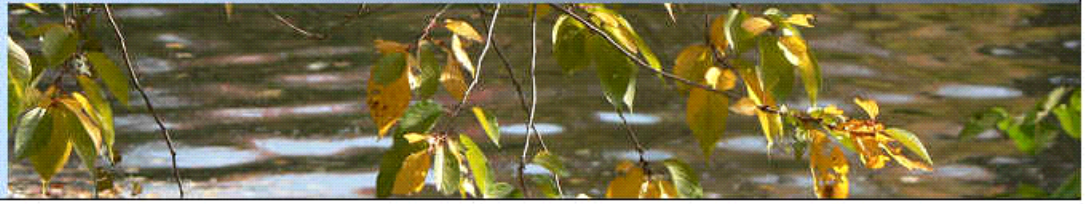
Nachteil: anfällig gegen Bedienerfehler (versehentliches Löschen). Das Betriebssystem und die Anwendungsprogramme (installierte Software) selbst können auf diese Weise nicht wieder hergestellt werden! Ferner werden die Einstellungen des Systems (wie z.B. Zugangscode, automatische Passwörter etc.) nicht gesichert.

Gefahr: viele Anwendungsprogramme (wie z.B. MS Outlook, StarMoney etc.) speichern ihre Daten in Ordnern ab, die dem Anwender selbst nicht direkt bekannt sind. Hier muss der Anwender entweder bei der Installation des Programms dieses sehr gut konfigurieren, oder regelmäßig (!) die Daten der Anwendungsprogramme separat (z.B. in „meine Dateien“) sichern.

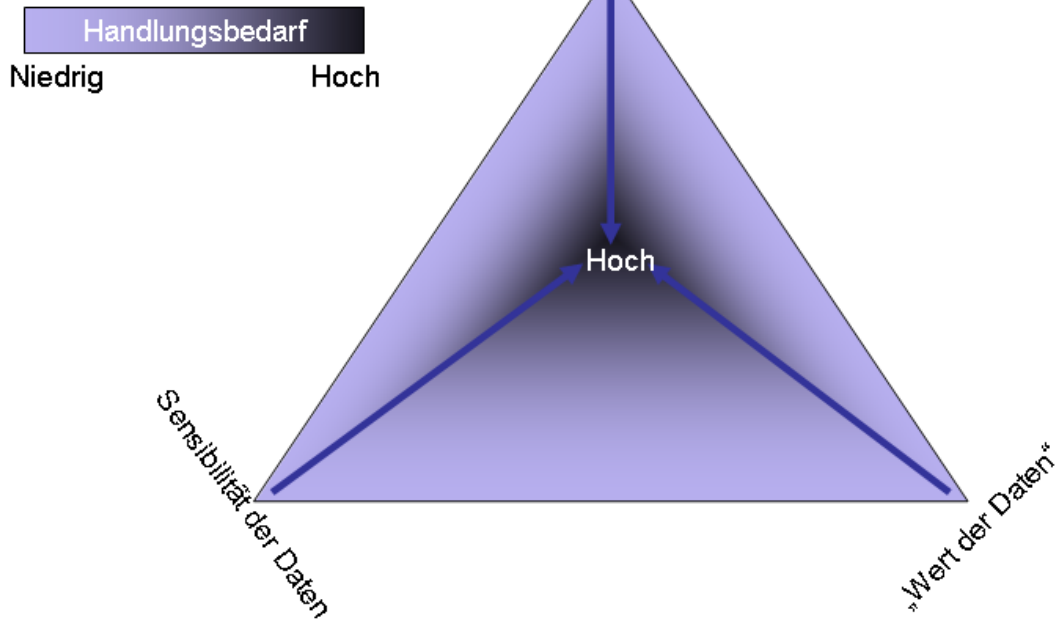
Wie sichern Sie Ihre Daten:

- Nur als Image der Festplatte?
- Nur als Sicherung der Anwender-Daten (Teilsicherung)?
- Als Kombination von Image und separater Sicherung der Anwender-Daten (Anwendungsprogramme (Software) sind zusätzlich im Original vorhanden)?
- Sind die Sicherheitskopien gegen unbefugte Verwendung (Diebstahl) ausreichend geschützt?

- **Entspricht Ihr Konzept zur Datensicherung dem Schutzbedürfnis / der Wichtigkeit Ihrer Daten?**
- **Setzen Sie Ihr Konzept zur Datensicherheit auch tatsächlich um?**
- **Dokumentieren Sie die erfolgte Umsetzung?**



Risiko - Bedrohungspotential



Hier finden Sie:

Fragen zum
Schutzbedürfnis
Ihrer Daten
Seite 2

Fragen zur
Sicherheit im
Interne und
e-Banking
Seite 6

Fragen zu Ihrem
Konzept zur
Datensicherheit
Seite 8

Über den Autor
Seite 10

Beim Beantworten der Fragen zu dem Schutzbedürfnis Ihrer Daten (Seiten 2 bis 5) sollte Ihnen bewusst geworden sein, wie wichtig und wertvoll Ihre Daten und Computerprogramme für Sie selbst sind. Zusätzlich sollten Sie jetzt abschätzen können, ob Sie sensible (für Dritte interessante) Daten auf Ihrem Rechner gespeichert haben.

Haben Sie die Fragen zur Sicherheit gegen Diebstahl (Seite 6 folgend) und zur Sicherheit gegen physikalischen Datenverlust (Seite 8 folgend) beantwortet, so sollten Sie eine Vorstellung über das Risiko bzw. das Bedrohungspotential gewonnen

haben. Lassen Sie ihren gesunden Menschenverstand walten und seien sie lieber etwas zu vorsichtig als zu optimistisch.

Je nachdem zu welcher Einschätzung Sie hinsichtlich Wert, Sensibilität und Risiko gekommen sind, ergibt sich entsprechender Handlungsbedarf. Im Zweifelsfall kontaktieren Sie einen entsprechenden Experten.

❖ Über den Autor

Dr. Hansgeorg Schaller, Promotion an der Universität Mainz in analytischer Chemie.

Langjährige Tätigkeit bei der Firma Chrompack als Chromatographiespezialist: Anwenderbetreuung,

Kurse in GC, HPLC, GPC, Fehlersuchetechniken, DIN/ISO 9001 Systeme sowie als Vertriebsleiter Deutschland.

Anschließend Konzentration auf das e-Business bei den Firmen eLabsEurope (Internet-Marktplatz) und ELEMICA (EDI-Plattform) als Sales Manager und Director Commercial Solutions.

Seit Anfang des Jahres 2005 tätig bei der SHE Informationstechnologie, spezialisiert auf Applikations-Sicherheit und Lösungen für Anwenderauthentisierung.

Weiteres Tätigkeitsgebiet: industrielle Lösungen zur Abwehr von SPAM-Mail. Des weiteren Projektbeauftragter für CRM.

Dr. Hansgeorg Schaller
<http://www.hg-schaller.de>
[post\(at\)hg-schaller.de](mailto:post(at)hg-schaller.de)

Bitte ersetzen sie (at) durch @!