

# Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Anstalt des öffentlichen Rechts

**Sommerakademie  
2017**

## **PCs, Tablets und Smartphones Umgang mit Schwachstellen und Risiken im praktischen Einsatz**

**Heiko Behrendt**

ISO 27001 Auditor

Fon: 0431 988 1212

Mail: [behrendt@datenschutzzentrum.de](mailto:behrendt@datenschutzzentrum.de)

Web: <https://www.datenschutzzentrum.de/>



Unabhängiges Landeszentrum für  
Datenschutz Schleswig-Holstein

## Themen

- Schwachstellen und Risiken ... bei mir auch?!
- Mindestanforderungen
- Checklisten
- „Live-Tools“

# Wie sicher ist Ihr Kennwort?



KeyGrabber

Hardware Keylogger - KeyGrabber PS/2

<https://www.keelog.com>



<https://www.heise.de>

# Jedes Kennwort kann geknackt werden?!

WIE SICHER IST MEIN PASSWORT?

.....

Ein herkömmlicher PC könnte dein Passwort innerhalb von  
**0.0011881376 Sekunden** knacken. ✨

(Der Seitenbetreiber gibt keine Gewähr auf die Angabe und deren Korrektheit.)

DEIN PASSWORT IST KURZ!

Je länger ein Passwort ist, desto sicherer ist es!

DEIN PASSWORT BESTEHT AUS SEHR WENIG ZEICHENSORTEN!

Versuche mit **Groß-** und **Kleinschreibung** sowie **Zahlen** und **Sonderzeichen** mehr Abwechslung in dein Passwort zu bringen!

MEHR INFORMATIONEN UND VIELE TIPPS...

... für ein sicheres Passwort findest du in unserem Leitfaden "Mein sicheres Passwort".

## Checkliste - Kennwortsicherheit

1. Ist für Kennwörter eine Mindestlänge von 8 Zeichen vorgegeben?
2. Werden für Kennwörter Sonderzeichen systemseitig erzwungen?
3. Wird ein Kennwortwechsel z. B. alle 90 Tage gefordert?
4. Werden die Kennwortrichtlinien für die Anmeldung am PC und die Anmeldung an Fachanwendungen analog umgesetzt?
5. Ist das Kennwort ausschließlich nur dem Nutzer bekannt?
6. Sind die Administrationskennwörter zusätzlich durch eine Zwei-Faktor-Authentifizierung (Token) abgesichert?
7. Wie werden die Kennwörter von Standardinstallationsbenutzerkonten geschützt?
8. Wird sichergestellt, dass auf den IT-Systemen und IT-Komponenten unterschiedliche Kennwörter der Standardinstallationsbenutzerkonten verwendet werden?
9. Gibt es ein Meldeverfahren für den Fall, dass Kennwörter Dritten bekannt werden?
10. Sind die Mitarbeiter im Umgang mit ihren Kennwörtern geschult?

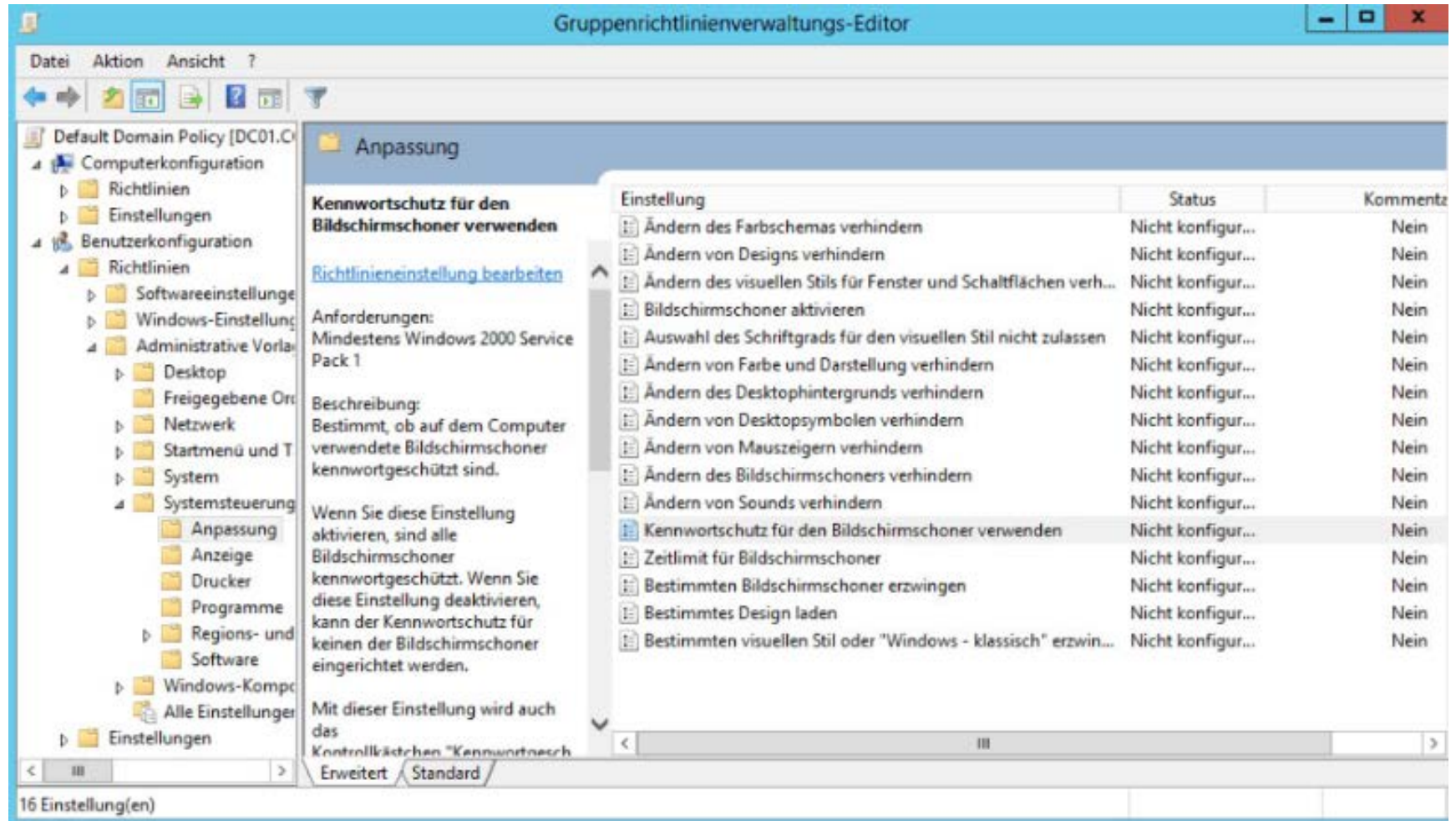
Soll-Ist-Abgleich heißt die Zauberformel ...  
... oder wie werden bei Ihnen die Befugnisse des  
Mitarbeiters auf Daten festgelegt und überprüft?



<https://pixabay.com>

# Gruppenrichtlinien-Verwaltungskontrolle

[https://technet.microsoft.com/de-de/library/cc753298\(v=ws.11\).aspx](https://technet.microsoft.com/de-de/library/cc753298(v=ws.11).aspx)



**Gruppenrichtlinienverwaltungs-Editor**

Default Domain Policy [DC01.C...]

- Computerkonfiguration
  - Richtlinien
  - Einstellungen
- Benutzerkonfiguration
  - Richtlinien
    - Softwareeinstellungen
    - Windows-Einstellungen
    - Administrative Vorlagen
      - Desktop
      - Freigegebene Ordner
      - Netzwerk
      - Startmenü und Taskleiste
      - System
      - Systemsteuerung
        - Anpassung
        - Anzeige
        - Drucker
        - Programme
        - Regions- und Sprachen
        - Software
        - Windows-Komponenten
        - Alle Einstellungen
        - Einstellungen

**Anpassung**

**Kennwortschutz für den Bildschirmschoner verwenden**

[Richtlinieneinstellung bearbeiten](#)

Anforderungen:  
Mindestens Windows 2000 Service Pack 1

Beschreibung:  
Bestimmt, ob auf dem Computer verwendete Bildschirmschoner kennwortgeschützt sind.

Wenn Sie diese Einstellung aktivieren, sind alle Bildschirmschoner kennwortgeschützt. Wenn Sie diese Einstellung deaktivieren, kann der Kennwortschutz für keinen der Bildschirmschoner eingerichtet werden.

Mit dieser Einstellung wird auch das Kontrollkästchen "Kennwortgesch..."

Einstellung	Status	Kommentar
Ändern des Farbschemas verhindern	Nicht konfigur...	Nein
Ändern von Designs verhindern	Nicht konfigur...	Nein
Ändern des visuellen Stils für Fenster und Schaltflächen verh...	Nicht konfigur...	Nein
Bildschirmschoner aktivieren	Nicht konfigur...	Nein
Auswahl des Schriftgrads für den visuellen Stil nicht zulassen	Nicht konfigur...	Nein
Ändern von Farbe und Darstellung verhindern	Nicht konfigur...	Nein
Ändern des Desktophintergrunds verhindern	Nicht konfigur...	Nein
Ändern von Desktopsymbolen verhindern	Nicht konfigur...	Nein
Ändern von Mauszeigern verhindern	Nicht konfigur...	Nein
Ändern des Bildschirmschoners verhindern	Nicht konfigur...	Nein
Ändern von Sounds verhindern	Nicht konfigur...	Nein
<b>Kennwortschutz für den Bildschirmschoner verwenden</b>	Nicht konfigur...	Nein
Zeitlimit für Bildschirmschoner	Nicht konfigur...	Nein
Bestimmten Bildschirmschoner erzwingen	Nicht konfigur...	Nein
Bestimmtes Design laden	Nicht konfigur...	Nein
Bestimmten visuellen Stil oder "Windows - klassisch" erzwin...	Nicht konfigur...	Nein

16 Einstellung(en)

<https://www.tecchannel.de/a/kennwoerter-per-richtlinien-regeln,3277616>

## Checkliste – Benutzerkonten, Benutzerprofile

1. Besteht für die Einrichtung, Änderung und Löschung von Benutzerkonten und Rechten ein nachvollziehbarer Prozess?
2. Werden Benutzerkonten und Rechte auf Anforderung der Fachabteilungen von der IT-Abteilung eingerichtet?
3. Können die Vorgaben (Soll) mit den Einstellungen am System (IST) überprüft werden?
4. Wird ein Revisionstool z. B. Dumpsec für die Auswertung der Benutzer- und Gruppenkonten eingesetzt?
5. Sind die Benutzerkonten personalisiert?
6. Kann festgestellt werden, über welche Rechte ein Mitarbeiter verfügt?
7. Werden Benutzerkonten nach mehrmaliger Falscheingabe des Kennworts gesperrt?
8. Ist bekannt, welche Administrationskonten auf welchen IT-Systemen bzw. IT-Komponenten vorhanden sind und verwendet werden?
9. Ist festgelegt, welche administrativen Benutzerkonten für welche Aufgaben und Dienstleister verwendet werden?
10. Werden die Benutzerkonten in Anwendungen analog verwaltet?



Löschen Sie Ihre Daten etwa nicht auf  
Nimmerwiedersehen?!



<https://pixabay.com>

# Auf Nimmerwiedersehen .... aber bitte physikalisch!

[HOME](#)[HELP](#)[DOWNLOAD](#)[FORENSIC NEWS](#)[ERASER-VIDEO](#)[FORUM](#)[Follow @heidi\\_eraser](#)

Erases files, folders and their previously deleted counterparts.

Eraser is Free software and its source code is released under GNU General Public License.

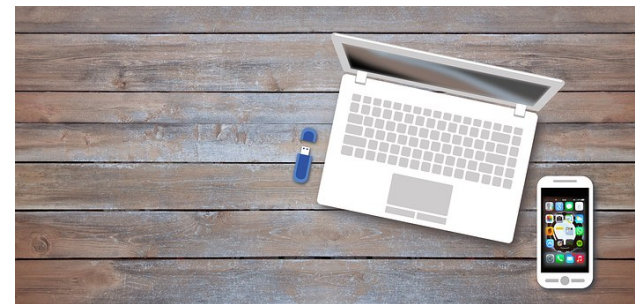


<https://eraser.heidi.ie/>

## Checkliste – Datenlöschung, Datenvernichtung

1. Sind von den Fachbereichen Löschfristen für die Datenverarbeitung festgelegt?
2. Ist bekannt, auf welchen IT-Komponenten welche Daten verwaltet bzw. gespeichert werden?
3. Wurden die Daten nach ihrer Sensibilität eingestuft?
4. Verfügen die eingesetzten Fachanwendung über Löschfunktionen entsprechend der festgelegten Löschfristen?
5. Können Dateien (Word, Excel) vom Nutzer physikalisch gelöscht werden?
6. Gibt es für mobile Datenträger (Smartphone, Tablet, Stick, Speicherkarte etc.) Regelungen zur physikalischen Löschung der Daten?
7. Werden Daten auf Datensicherungsmedien gelöscht?
8. Wie werden bei Aussonderung von IT-Systemen die verbauten Datenträger vernichtet oder physikalisch gelöscht?
9. Werden auch Akten analog zu digitalen Daten vernichtet?
10. Sind für die Vernichtung der Daten die Regelungen der DIN 66399 bekannt?

# Haben Sie Ihre Daten noch unter Kontrolle?!

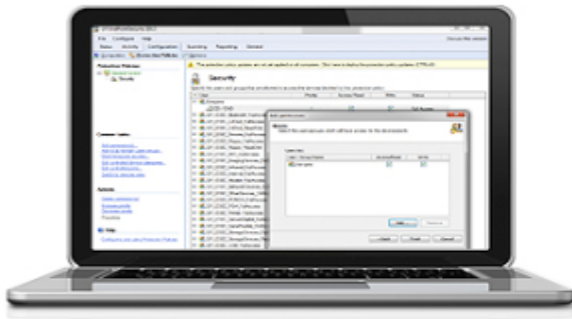


<https://pixabay.com>

# Sicherheitssoftware für mobile Datenträger

**GFI EndPointSecurity**

<https://www.gfisoftware.de>



Einfache Steuerung des Zugriffs auf mobile Datenträger

Legen Sie zentral fest, in welchem Zeitraum ein Datenaustausch zwischen mobilen Datenträgern und Computern in Ihrem Netzwerk gestattet sein soll. Blockieren Sie Inhalte unter Berücksichtigung ihrer Dateierweiterung. Oder sperren Sie Mobilgeräte nach Hardware-Kategorie, Schnittstelle und Seriennummer.

Produktauszeichnungen



## Alternativ

<https://www.devicelock.com/de/>

<https://drivelock.de>

## Weitere Vorteile

### Dateikontrolle

Überprüfen Sie den Inhalt von Archivdateien, und blockieren Sie Dateien abhängig von ihrer Größe.

### Detaillierte Berichterstellung

Lassen Sie sämtliche Aktivitäten lückenlos erfassen und automatisch in täglichen oder wöchentlichen Berichten protokollieren.

### Automatischer Schutz

Neue Computer sind durch die umgehende Installation eines Agenten samt standardmäßiger Schutzrichtlinie automatisch geschützt.

### Zentrale Überwachung

Informieren Sie sich über alle in Ihrem Netzwerk erkannten Computer und damit verbundene mobile Datenträger.

## Checkliste – USB-Sticks, Speichermedien

1. Werden die Schnittstellen des PCs und der mobilen IT-Systeme unter Einsatz einer Sicherheitssoftware reglementiert?
2. Sind mobile Datenträger, z. B. Sticks u. Speicherkarten, inventarisiert?
3. Ist es untersagt, private IT-Systeme und Datenträger einzusetzen?
4. Werden die Daten auf mobilen Datenträgern verschlüsselt gespeichert?
5. Sind die Konfiguration der Verschlüsselung und die Behandlung von Kennwörtern durch die IT-Abteilung vorgegeben?
6. Ist festgelegt, welche Daten auf mobilen Datenträgern gespeichert bzw. genutzt werden dürfen?
7. Soll ggf. protokolliert werden, welche Dateien zwischen mobilen Datenträgern und internen IT-Systemen transferiert werden?
8. Ist bekannt, dass auf den Speichermedien logisch gelöschte Dateien einfach rekonstruierbar sind?
9. Gibt es bei Verlust von mobilen Datenträgern ein Meldeverfahren?
10. Sind die Mitarbeiter über den Umgang mit mobilen Datenträgern ausreichend sensibilisiert und geschult?

Smartphone: Gibt es da ein Problem?!



<https://pixabay.com>

# Sicherheitssoftware für mobile Datenträger

Beispiele für Sicherheitseinstellungen:

- Übermittlung von Diagnosedaten sperren
- Kennwortrichtlinien aktivieren
- Nutzung des App Stores reglementieren
- Organisationsbezogene Apps festlegen
- Verschlüsselung der Speicher aktivieren
- Änderungen an den App-Einstellungen sperren
- Privaten Hotspot sperren
- Clouddienste sperren
- ...

**CITRIX**  
**XenMobile**



**Sophos Mobile**  
**Control**



## Checkliste – Notebook, Tablet und Smartphone

1. Wird eine Mobile-Security-Management-Software für die zentrale Administration der mobilen IT-Systeme eingesetzt?
2. Wurden die für IT-Systeme geltenden Sicherheitsanforderungen von den Verantwortlichen festgelegt und können diese in Form von technischen Maßnahmen umgesetzt werden?
3. Wird sichergestellt, dass nur von der Organisation freigegebene Programme/Apps genutzt werden können?
4. Werden die Daten verschlüsselt gespeichert?
5. Sind die IT-Systeme ausreichend vor Viren geschützt?
6. Wird sichergestellt, dass Daten nicht unbemerkt ausgelesen werden?
7. Werden die Schnittstellen USB, WLAN und Bluetooth abgesichert?
8. Wird ein Jailbreak bzw. ein Rooten der IT-Systeme verhindert?
9. Kann das IT-System ggf. bei Verlust per Fernzugriff deaktiviert bzw. können die auf dem IT-System gespeicherten Daten gelöscht werden?
10. Werden sicherheitsrelevante Updates und Patches installiert?

## 10 wichtige Schutzmaßnahmen

1. Verfügen die Nutzer über **keine** administrativen Berechtigungen?
2. Werden Kennwort- und Kontosperrungsrichtlinien **angemessen** umgesetzt?
3. Sind die Schnittstellen für mobile Datenträger auf das **erforderliche Maß** reglementiert?
4. Verfügen die Systeme über **aktuelle** Betriebssystemupdates und Antivirensoftware?
5. Werden die „Gruppenrichtlinien“ für die **Beschränkung** der Desktopfunktionen eingesetzt?
6. Können Dateien (Word, Excel etc.) **physikalisch** gelöscht werden?
7. Sind die Daten auf den mobilen Datenträgern **verschlüsselt**?
8. Ist die Datenkommunikation über **Datennetze** (Internet, WLAN, Bluetooth) geschützt?
9. Werden Daten **zentral** auf internen Speichersystemen verwaltet bzw. synchronisiert?
10. Wird ein Backup auf **Datensicherungsmedien** von Administratoren durchgeführt?

# PCs, Tablets und Smartphones

## Umgang mit Schwachstellen und Risiken im praktischen Einsatz

**Vielen Dank für Ihre Aufmerksamkeit!**

**Heiko Behrendt**

ISO 27001 Auditor

Fon: 0431 988 1212

Mail: [behrendt@datenschutzzentrum.de](mailto:behrendt@datenschutzzentrum.de)

Web: <https://www.datenschutzzentrum.de/>