G. Umgang mit Datensicherheit

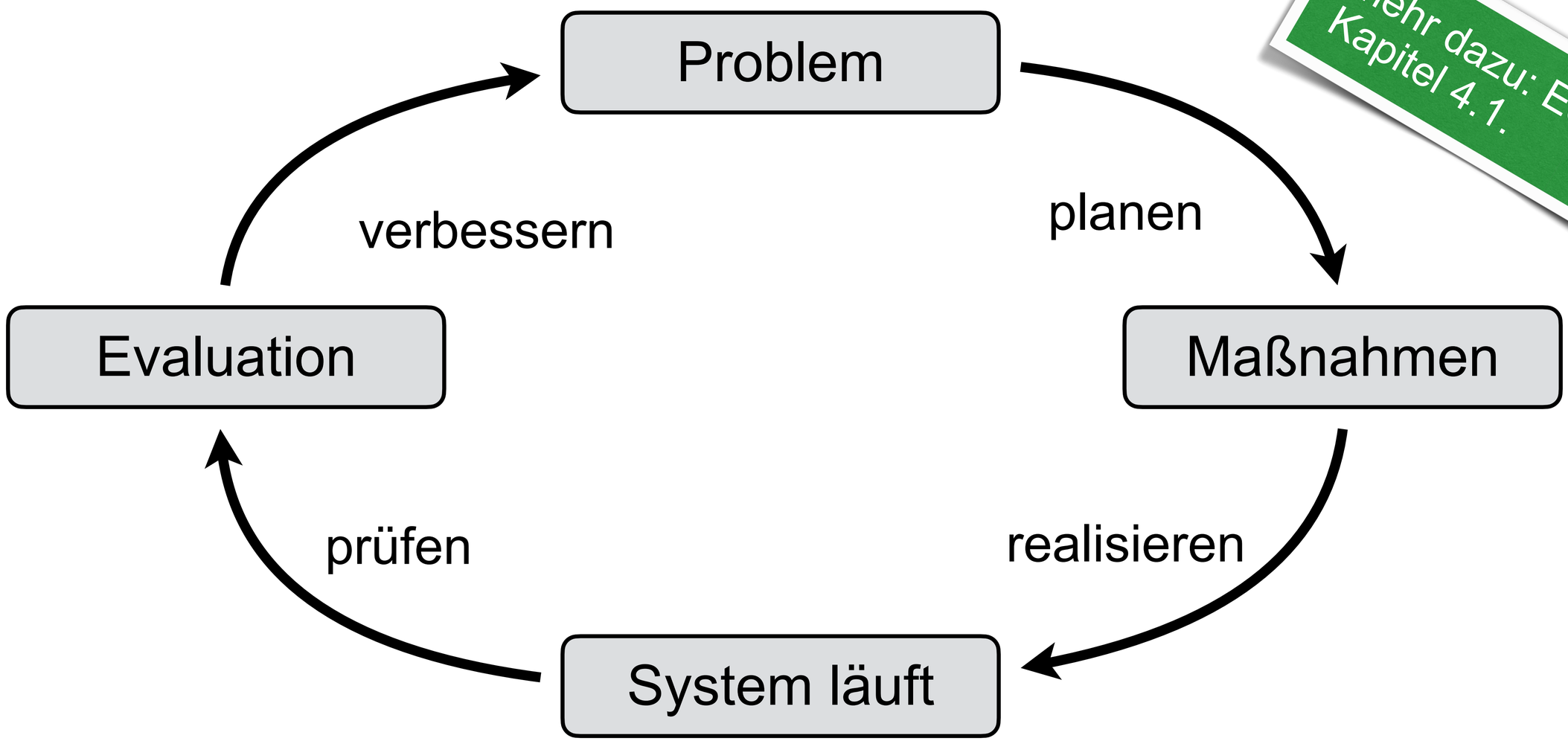
Was wollen und können wir erreichen?

- 100-prozentige Sicherheit ist nicht möglich - möglich sind:
  - möglichst hohe, im konkreten Fall angemessene Sicherheit,
  - gute Vorbereitung auf den Ernstfall! => Resilienz

- konkreter Plan:
  1. wie geht *security engineering*?
  2. welche Techniken / Lösungen und wie einsetzen?
  3. welche Vorgehensweisen und Strategien sind erfolgreich?

G.1. Sicherheitsprozess - kontinuierliche Verbesserung

Management - Phasen eines sicheren Systems / PDCA



mehr dazu: Eckert, Kapitel 4.1.

In Anlehnung an Eckert, IT-Sicherheit, Kapitel 4.1.2

G.1. Allgemeine Regeln aus technischer Sicht

Konstruktion sicherer Systeme - Prinzipien

Erlaubnisprinzip	▸ *default deny* ▸ grundsätzlich ist jeder Zugriff verboten
Vollständigkeit	▸ jeder Zugriff ist zu prüfen ▸ nicht nur z. B. beim Öffnen der Datei…
need to know	▸ was muss ein Benutzer zwingend wissen? ▸ jeder nur die Rechte, die er zwingend braucht…
Akzeptanz	▸ Sicherheitsmechanismen akzeptabel ▸ vor allem automatisch!
Offenheit	▸ Verfahren / Mechanismen der Sicherheit transparent ▸ *no security through obscurity*

G.1. Vorgehensweise

die wichtigsten Schritte

- relevante Systemeigenschaften erfassen
- Schutzbedarf ermitteln
  - d. h. Schäden ermitteln, die auftreten können
- Bedrohungen (die solche Schäden bewirken können) erfassen
  - Bedrohungs- und Risikoanalyse
- Sicherheitsstrategien, **Sicherheitsarchitektur** schaffen
- Sicherheitsgrundfunktionen => Leitlinien (d. h.: dokumentiert)

- Beispiel Softwareentwicklung: SDL (Security Development Life-cycle)

G.1. Vorgehensweise

Dokumentation und ihre Rolle

Vgl. Kersten / Klett:
Der IT Security Manager,
Kapitel 3.3

G.2. Methoden und Werkzeuge

Systematik

- Verträge und andere Regelungen
- Organisation
- Personal
- Infrastruktur
- Technik

Wichtig: Validierung!

G.2.c. Methoden und Werkzeuge

Technische Maßnahmen

- **Backup - aber richtig**
- Lücken minimieren - Security Updates
- Vertraulichkeit mit Verschlüsselung
- Ins Netz gehen - der Router und nicht nur
- Heterogenität und Isolation
- Analyse und Überwachung

G.2.c. Methoden und Werkzeuge - Technik

Technische Maßnahmen - Backup

- **die Notwendigkeit - wohl triviale Feststellung…**
- einfach: nur automatisches Backup wird nicht vergessen
- darf nicht angreifbar sein - besonderer Schutz!
- gesicherte Daten müssen transparent, gut auffindbar sein
- Wiederherstellung muss regelmäßig getestet werden
- Analyse und Überwachung
- System insgesamt robust (eine HDD kann auch kaputtgehen)
- standortunabhängig? => Replikation

Achtung: Backup schützt nicht vor Verletzung der Vertraulichkeit!

G.2.c. Methoden und Werkzeuge - Technik

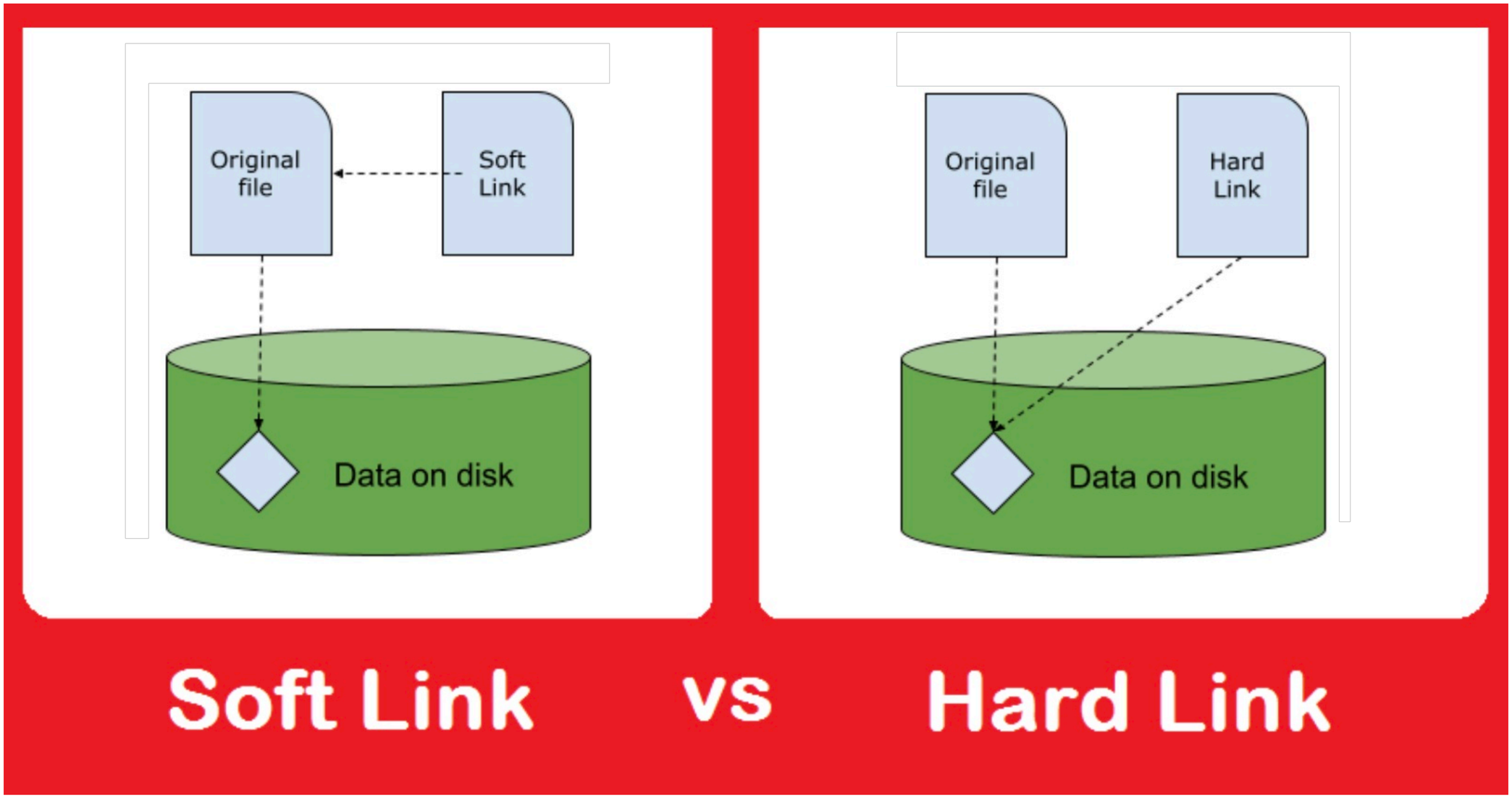
in wenigen Schritten zum einfachen rsync-Backup

- Verbindung zwischen den Rechnern ermöglichen => SSH
  - Zertifikate erstellen und austauschen
- script einrichten
  - Dateien per rsync / ssh holen
  - inkrementelle Kopie mit Hardlinks erstellen
- CRON-job einrichten (regelmäßige, automatische Ausführung)

funktioniert auf allen UNIX-artigen Systemen, auf Umwegen auch unter Windows (Sicherung aber auf einem UNIX-Dateisystem!)

G.2.c. Methoden und Werkzeuge - Technik

rsync-Backup - Hardlinks besonders hilfreich!



G.2.c. Methoden und Werkzeuge - Technik

Beispiel eines ausgereiften Werkzeugs: TrueNAS

- einfache Einrichtung und Bedienung über Web-Oberfläche
  - dadurch korrekte Bedienung teils zumindest erzwungen
- hohe Sicherheit mit bewährtem FreeBSD
  - UNIX-Betriebssystem mit klarem Sicherheitskonzept
- ZFS-Dateisystem mit Snapshots, Replikation etc.
  - fortschrittlichstes Dateisystem der Welt
- robustes System, aktive Community, professionelle Funktionen

Alternativen: Proxmox mit ZFS, Debian/Ubuntu mit btrfs und rsync etc.; kommerziell: Solaris von Oracle

G.2.c. Methoden und Werkzeuge - Technik

Verschlüsselung zur Wahrung der Vertraulichkeit

Datenträger-verschlüsselung	- mobile Geräte - Datenträger, die gestohlen werden können
Kommunikation	- WWW: https ist zwingend! - E-Mail - jedenfalls TLS zwischen Client/Server - je nach Szenario => auch Nachrichten selbst! - sonstige Protokolle: ‣ Administration - SSH ‣ FTP => SFTP
Netzwerk-verbindung	Hinreichend verschlüsseltes VPN - auf keinen Fall über offene Ports (darüber hinausgehend) kommunizieren!

G.2.c. Methoden und Werkzeuge - Technik

Der Weg ins Netz: Router

Fritz!Box

Lancom

Fortinet etc.

OPNsense
pfsense
und andere OS-Lösungen

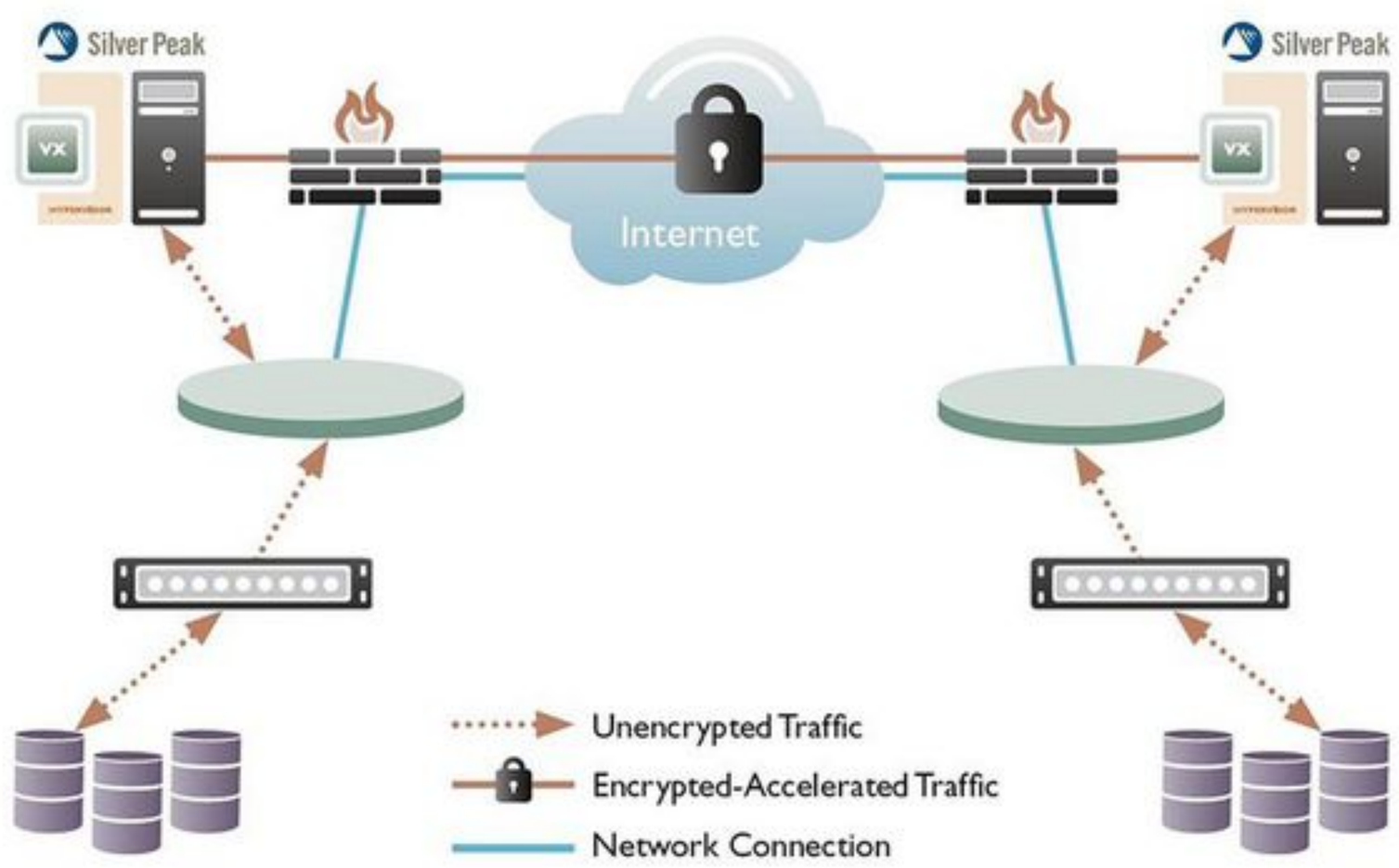
Möglichkeiten der konkreten Lösung sind an die Bedürfnisse des Netzwerkes anzupassen - OSS ist dabei am flexibelsten…

G.2. Methoden und Werkzeuge

Lösungen für VPN + Replication + Firewalls + WAN-Acceleration

Zahlreiche Anbieter:

- riverbed
- silverpeak
- wanos (reine Beschleuniger)
- veeam (speziell für Replikation)



Quelle: https://www.ip-insider.de/software-fuer-site-to-site-vpns-und-wan-beschleunigung-a-432751/

G.2. Methoden und Werkzeuge

Trusted Computing

- Sicherheit in fremden Händen
- Nutzbarkeit der Technik eingeschränkt
- Regierungen, Geheimdienste, Monopole?

vs.

Zero Trust

- Grundprinzip - man darf niemandem trauen
- deshalb: stetige Aufmerksamkeit
- Zugriff / Kommu-nikation immer von Schutzmechanismen flankiert

G.3. Allgemeine Empfehlungen

Einige strategische Überlegungen

- Konzepte sind wichtig - jedenfalls genaue Überlegungen!
- Technische Zuverlässigkeit
- keep it simple
- open source vs. closed source
- Absicherung vs. Resilienz

kein „Allheilmittel“, können aber im richtigen Moment die Entscheidung erleichtern

G.3.a. Konzepte, Integrierte Systeme

ISMS

verinice ist ein ISMS-Tool für das Management von Informationssicherheit. Die Software steht unter der Lizenz GPLv3 zum Download als OpenSource-Software bereit.

verinice eignet sich:

- zur Implementierung von **BSI IT-Grundschutz**
- für den Betrieb eines **ISMS nach ISO 27001**
- zur **Risikoanalyse nach ISO 27005**
- für ein **Information Security Assessment (ISA)** nach VDA-Vorgaben
- allgemein für die Arbeit mit den folgenden Standards: ISO 27001, ISO 27002, ISO 27005, ISO 27018, ISO 27019, ISO 27004, BSI 100-1 bis -4, PCI DSS, COBIT, BDSG, EU DSGVO, SSAE 16, BCBS 239, ISAE 3402, MaRisk-E, SREP, VDA ISA, IDW PS 330, IDW PH 9.330.1

verinice unterstützt die Betriebssysteme Windows, Linux und macOS und hat die Grundschutzkataloge des BSI lizenziert.

Alle relevanten Standards sind entweder im Tool vorhanden oder können einfach implementiert werden. Alle Daten inkl. aller erstellten Dokumente sind in einer Objekt-Datenbank abgelegt, die an die Anforderungen von IS-Management angepasst ist und dynamisch erweiterbar ist.

G.3.e. Absicherung vs. Resilienz

Nicht nur Umsetzen, sondern auch testen!

- Beispiel Backup:
  - wie kompliziert ist die Wiederherstellung,
  - wie lange dauert sie,
  - was ist für den Fall der Fälle sonst zu bedenken,
  - was ist eventuell beim Sicherungsvorgang zu optimieren.

- auch sonst (Konzepte, Krisenmanagement) gilt:
  ohne Testlauf kein Verlaß auf die Wirksamkeit einer Lösung!