SENIOREN BERATEN
DIE WIRTSCHAFT

Datensicherheit für (jedes) Unternehmen

SENIOREN BERATEN
DIE WIRTSCHAFT

Inhalt

1. Was ist „Datensicherheit“?

2. Fall-Beispiele:
   Bedrohungen und Gegen-Maßnahmen

3. Grundlagen eines Backup-Konzepts

4. Vorschlag zur weiteren Vorgehensweise

Was ist „Datensicherheit“ …

Informationen:
Anfragen, Aufträge,
Planungen, Ideen,
Rechnungen,
Zahlungen

Ergebnisse:
Angebote,
Abrechnungen,
Auswertungen,
Produktionsaufträge

„Störungen“ + Gefahren:
Hardware-/Software-Fehler,
Ausfall von Übertragungswegen,
Fehlbedienungen („Löschen“),
Angriffe von außen („Hacker“),
Angriffe von innen,
Naturkatastrophen

… in Ihrem Unternehmen?

Einfach gesagt:

- Datensicherheit trägt dazu bei, dass Ihr Unternehmen arbeitsfähig ist + bleibt
- Datensicherheit ist eng verknüpft mit Unternehmens-Organisation und -Abläufen
- Wissen Sie, wie lange Ihr Unternehmen ohne funktionierende IT auskommt ???

1. Fall-Beispiel:

Hardwareausfälle

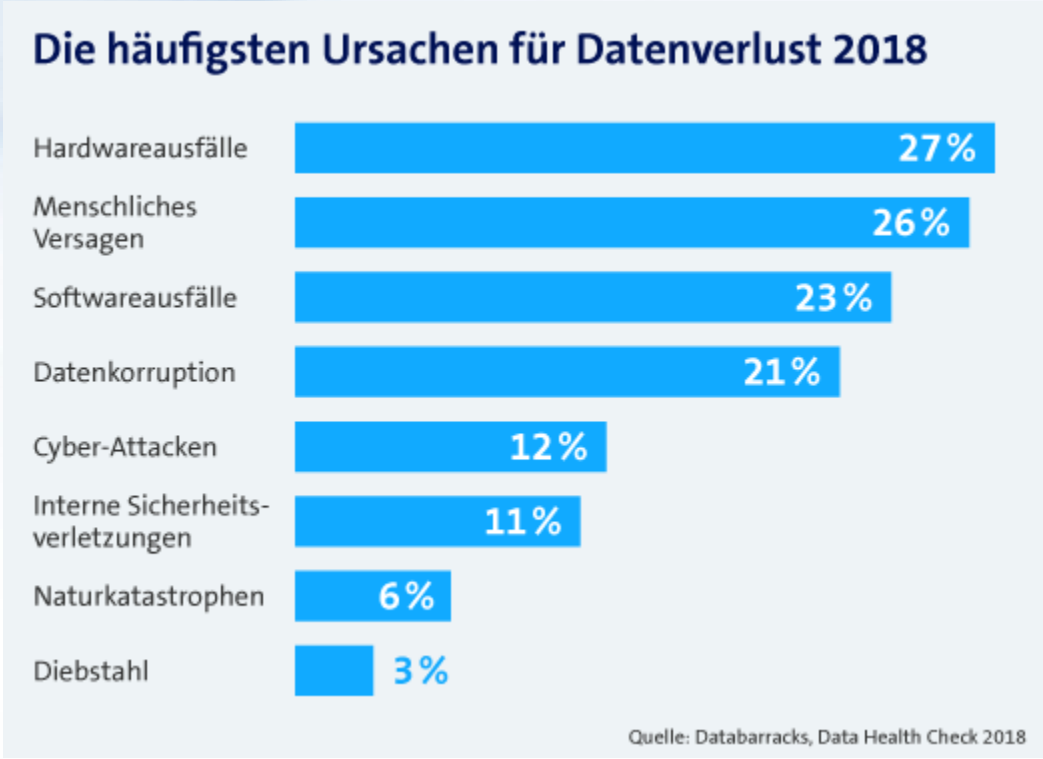
- Verschleiß (Festplatten altern, SSDs ebenso)
- Mechanische oder elektrische Defekte
  (z.B. durch Sturz, Überspannung, Netzteile!)

Menschliches Versagen

- Versehentliches Löschen/Ändern von Daten

Softwareausfälle

- Programm-Abstürze während der Verarbeitung

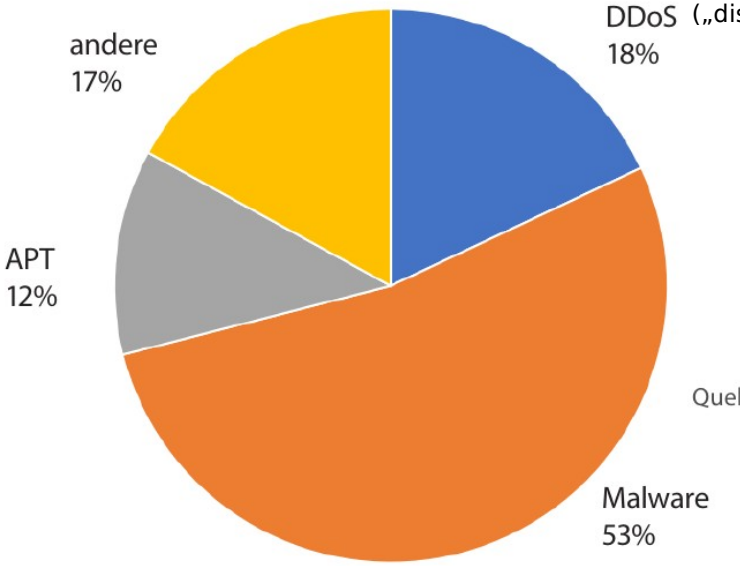


(Mehrfach-Nennungen waren möglich)

Cyber-Kriminalität oder interne Sicherheitsverletzung

- Phishing, Hacker-Angriffe, Ransom-Ware (Daten-Verschlüsselung + Erpressung)
- Absichtliches Löschen / Beschädigen („Rache-Akte“), Zugriffe nach Mitarbeiter-Kündigung, Daten-Diebstahl

2. Fall-Beispiel: Welche Angriffs-Arten kommen aktuell wie häufig vor?



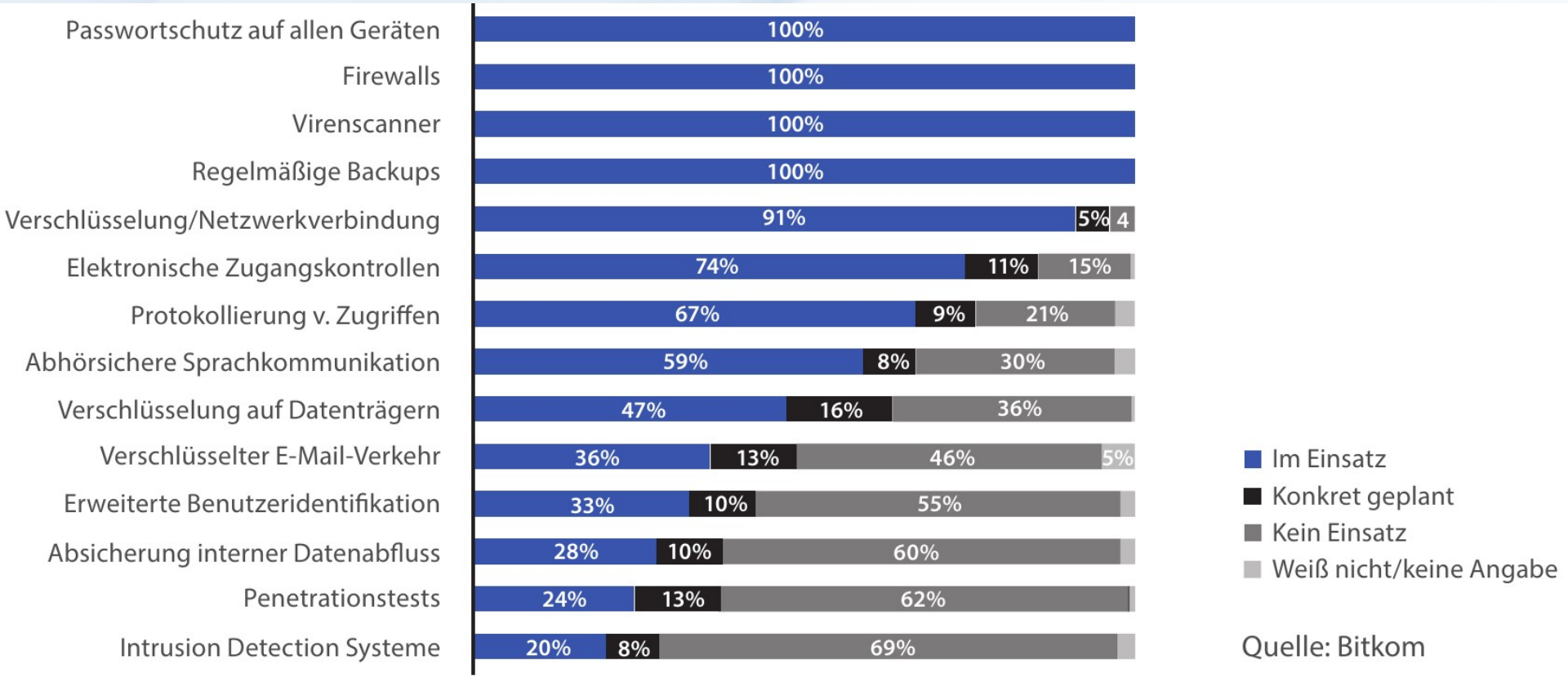
Quelle: Allianz für Cybersicherheit, BSI

Anteile in Prozent an allen berichteten Angriffen

Erläuterungen hierzu:

- Malware: in 90% der Fälle dienen Anhänge oder Links in E-Mails als Einfallstor. Abhilfe: durch Scanner + Schulung!
- DDoS: zielt auf die Überlastung von Servern oder Verbindungen → starke Beeinträchtigung der Geschäftsprozesse!
- APT (Advanced Persistant Threat): gezieltes Hacking zur Spionage oder Sabotage → meist hoher technischer Aufwand!

Welche technischen Abwehrmaßnahmen kommen bei KMU zum Einsatz? [2021]



Im Falle eines Angriffs / Datenverlusts: **in 99% der Fälle ist eine Daten-Wiederherstellung der richtige Weg!!**

Grundlagen eines (einfachen) Backup-Konzepts:

Ermittlung und Bewertung der eigenen Anforderungen

- Welche IT Systeme sind zu schützen, um welche Daten geht es?
- Welche (Geschäfts-)Prozesse hängen von den Systemen + Daten ab?
- Wie aktuell müssen im Notfall die wiederhergestellten Daten sein?
  - = **Menge/Zeitspanne der Daten, die verloren gehen dürfen** (RPO, Recovery Point Objective)
- Wie lange darf die im Notfall erforderliche Wiederherstellung maximal dauern?
  - = **Zeitraum bis „die IT“ nach dem Notfall wieder verfügbar ist** (RTO, Recovery Time Objective)
- Wie lange müssen gelöschte Daten wiederherstellbar sein? (=Backup-Historie, kein Archiv!)

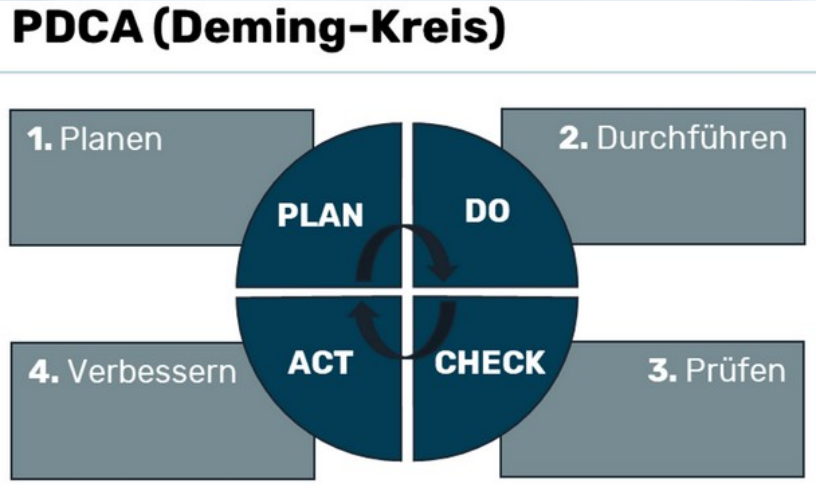
Auswahl / Festlegung einer „Backup-Strategie

- „High-Level“ Beschreibung: was, wie, wo, worauf/wohin, wie oft, wie lange, durch wen

Implementierung, Test und Dokumentation der Backup-Verfahren

- Auswahl und Beschaffung benötigter Backup-Hardware + -Software
- Backup und Restore probeweise durchführen und dabei dokumentieren (auch: benötigte Zeit)
- Backup-Konzept und Backup-/Restore-Verfahren mehrfach ausdrucken (und verteilen)

Vorschlag zur Vorgehensweise:



Die Partner der SBDW können Sie dabei sehr gerne unterstützen!

vorab: Bestandsaufnahme

Haben Sie einen dokumentierten Überblick über Ihre Prozesse und die IT-Systeme?

→ **erstellen/aktualisieren**

Risiko-Ermittlung:

welche Prozesse & Systeme sind unverzichtbar?

→ **bewerten + priorisieren**

Ableitung konkreter Maßnahmen:

wodurch kann das Risiko verringert werden?

→ **Maßnahmen umsetzen („Chefsache“)**

Zielkontrolle:

Maßnahmen testen, Erfolg bewerten

→ **regelmäßige Verbesserung planen**

SENIOREN BERATEN
DIE WIRTSCHAFT

Vielen Dank für Ihre Aufmerksamkeit

WORLD BACKUP DAY

jedes Jahr
am 31. März:

Seien Sie dabei!

https://www.worldbackupday.com/de