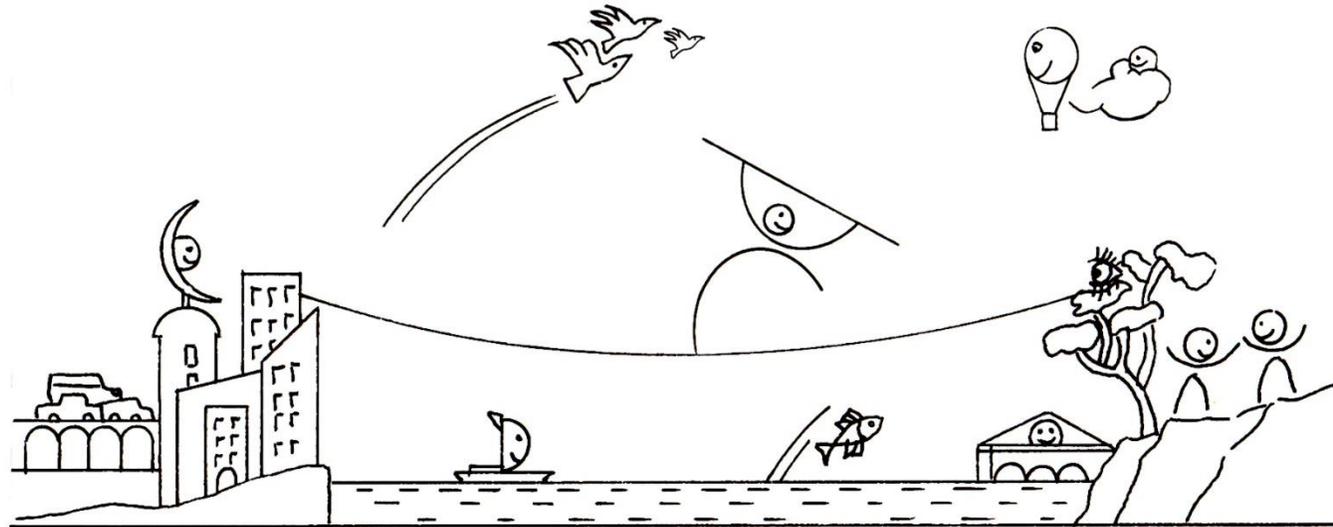




ENCRYPTION
EUROPE



Herzlich willkommen



Gibt es einen Datenairbag? Antiransomware – ein moderner Ansatz

Moderatoren : Beatrice Lange und Marc Wernscheid

Datum : 17.05.2022

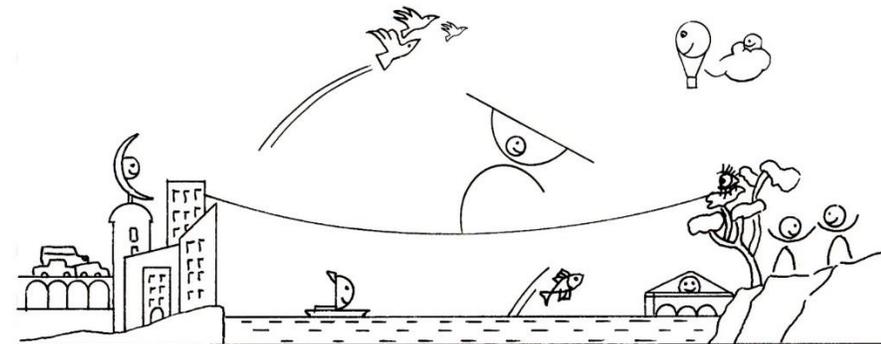
tetraguard systems GmbH

Wir sind führender Anbieter von Hard- und Software im Bereich IT-Security

Bekannt wurden wir durch die Entwicklung von IT-Security-Produkten für Microsoft Windows® Plattformen

Unsere Software ist frei von Drittprodukten
Alle Produkte garantiert frei von Backdoors

Enjoy Your Security Balance



Die Bedrohungen

➤ 9 von 10 Unternehmen* werden angegriffen,
z.B. KMU, Gesundheit, KRITIS, öffentlicher Sektor, Freie Berufe

und es kommt zu

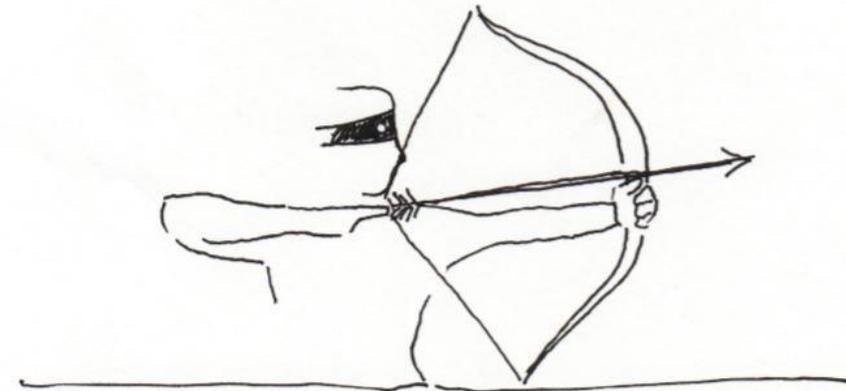
- Datendiebstahl
- Fremdverschlüsselung
- Spionage
- Sabotage
- Schäden durch Ransomware



* Quelle: BSI

Die Ziele von Cyberattacken

- Erpressung von Lösegeld
- Datendiebstahl, Fremdverschlüsselung
- Identitätsdiebstahl
- Abgreifen von Firmen-Know-How
- Kopieren von Behördenstrukturen
- Erlangung von Finanzdaten (Kreditkarten, Online-Banking...)
- Sabotage



Die Angreifer

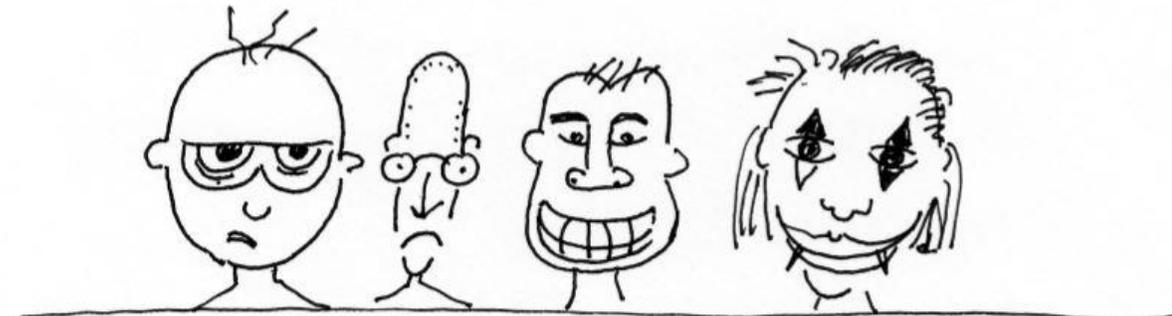
Abhängig von ihrer Motivation und ihrer Gesetzestreue lässt sich zwischen verschiedenen Typen von Hackern unterscheiden.

Die wichtigsten Hackertypen sind:

- White-Hat Hacker
- Grey-Hat Hacker
- Black-Hat Hacker

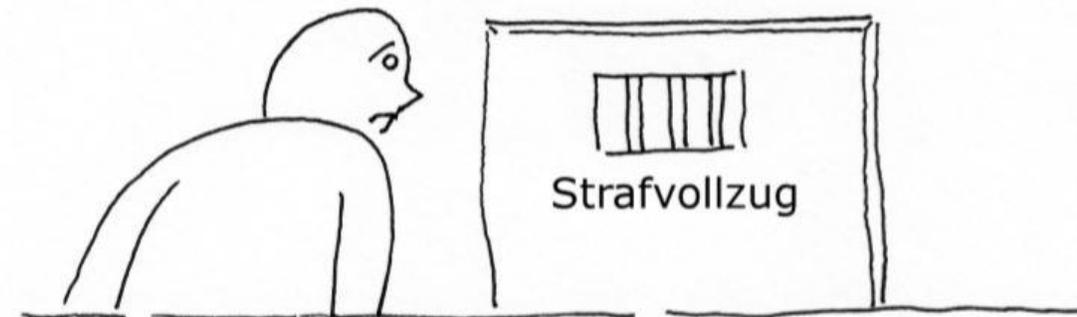
sowie:

- Geheimdienste



Die Schadensbilanz

- Über 20%*, der durch einen Cyberangriff betroffenen Unternehmen, musste Insolvenz anmelden!
- Weitere 15* Prozent mussten erhebliche Umsatzverluste hinnehmen
- Schadensumme 223 Mrd. EURO im Jahr 2021**
- Image- und Kundenverlust durch Vertrauensverlust und Lieferverzug



* Quelle: digitaleweltmagazin

**Quelle: Bitkom

aktuelle Schutzmaßnahmen

- aktueller Antivirenschutz
- Patch-Verwaltung / Patch-Management
- konsequente Backup-Strategie

- Mit diesen Maßnahmen ist eine wirkungsvolle Datensicherheit nur eingeschränkt möglich!



Die neue Lösung

Eine KI unterstützte Formel mit ihrem neuen Denkansatz

- + Starke 2FA
- + Dateibasierte Verschlüsselung
- + Application-Control

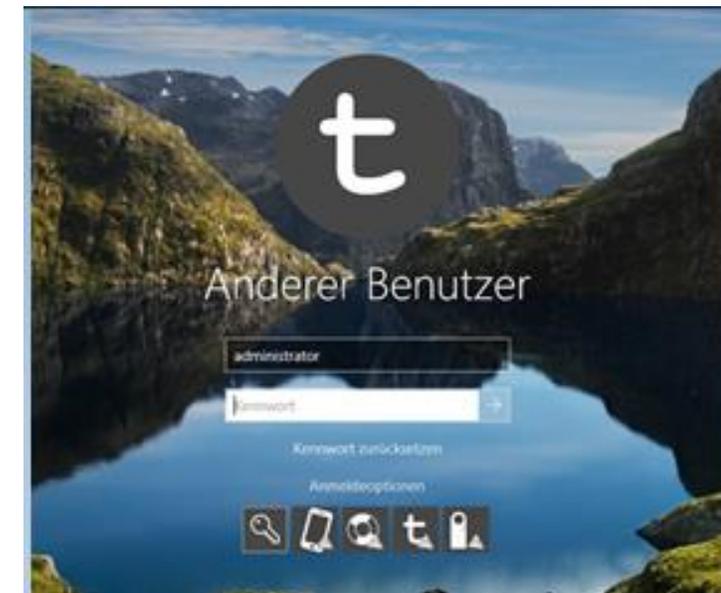
= wirksamer Schutz vor Ransomware

Alleinstellungsmerkmal Daten-Airbag



Authentifizierung

- zwei-Faktor-Authentifizierung
- mit oder ohne Hardwareanker – z.B. Token
- sicherer Schlüsselzugang
- Single-SignOn



Dateibasierte Verschlüsselung

- Daten können nur mit individuellen Schlüsseln gelesen und bearbeitet werden
- Ransomware verfügt **NICHT** über den passenden Schlüssel
- Auch nicht mit Admin-Rechten

= Schadsoftware prallt einfach ab



Application Control

- KI-gestützte Anwendungsüberwachung
- Anti-Ransom Technologie
- Maßgeschneiderter Dateizugriff
- Alarmierungskonzepte

Einstellungen / Übersicht



Die ausgewählte Einstellung

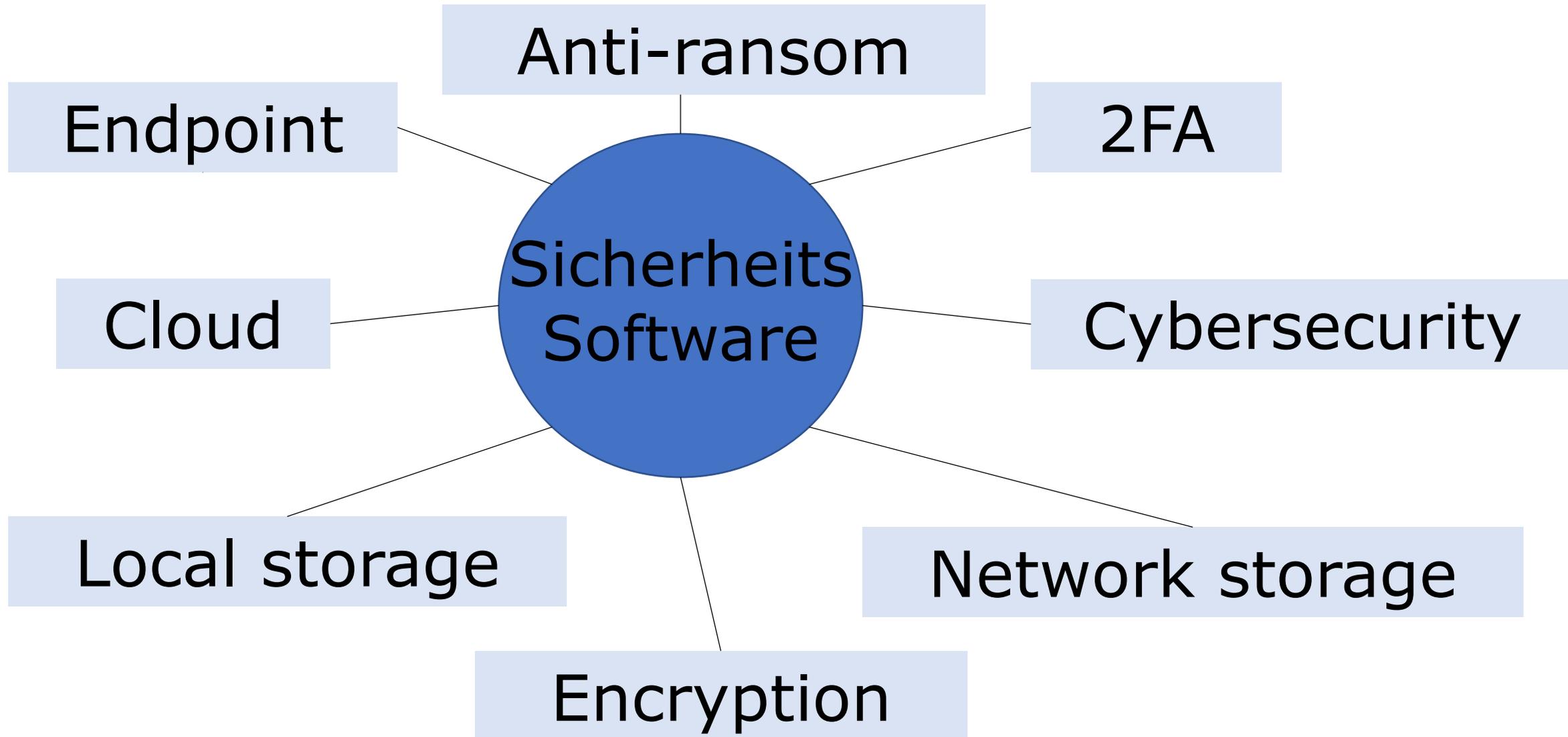
- stellt sicher, dass das Betriebssystem seine normalen Funktionen ausführen kann.
- schützt Ihr System vor unbekanntem Programmen.
- schützt Ihr System vor ungewünschter Modifikation durch Systemprozesse.
- schützt Office Dokumente.
- beschränkt die Einstellungsmöglichkeiten von Windows.
- schützt Multimedia Dateien aller Art.

Keine Ausnahmen für [Benutzer und Gruppen](#) vorgesehen.

Keine Ausnahmen für [Programme](#) vorgesehen.

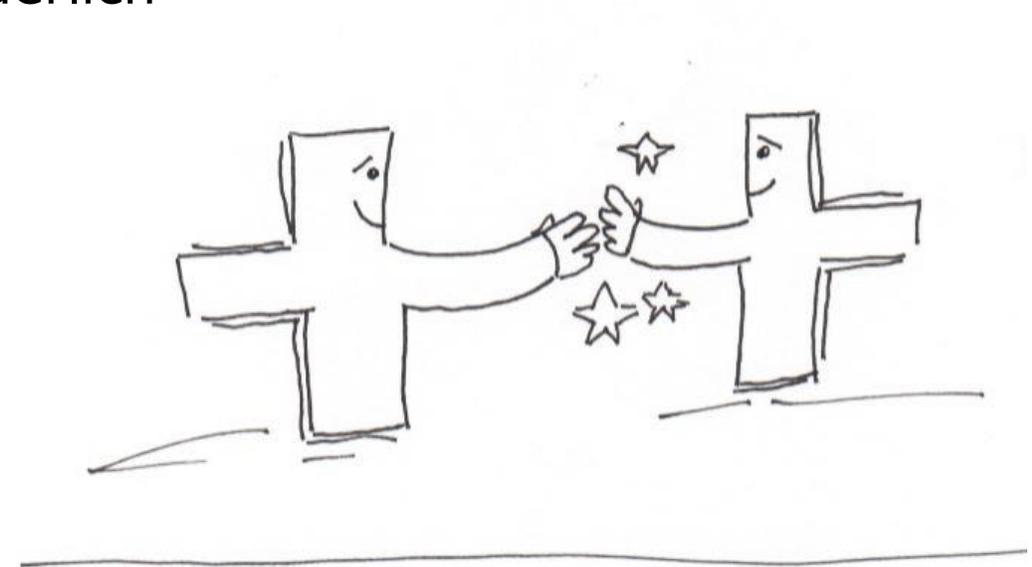
Keine Ausnahmen für [Token](#) vorgesehen.

Ihr Plus an Sicherheit



Pluspunkte einer guten Sicherheits-Software

- Keine aufwändigen Systemvoraussetzungen
- einfache Anwendung, keine Interaktion notwendig
- Möglichst keine Schulung für Mitarbeiter erforderlich
- Virtualisierungskonform



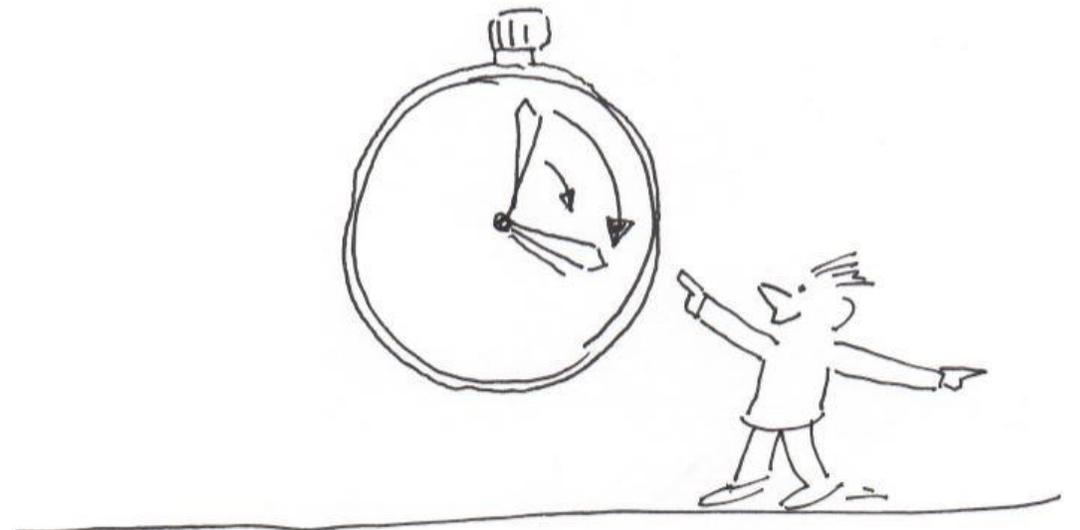
Datensicherheit – Ihr Nutzen

Hilfe gegen:

- Cyberattacken
- Datendiebstahl
- finanzielle Schäden

plus:

- Sicherstellung Ihrer Reputation
- Risikotransparenz
- nachvollziehbare Sicherheitstiefe
- Datensicherheit durch Verschlüsselung



Zusammenfassung

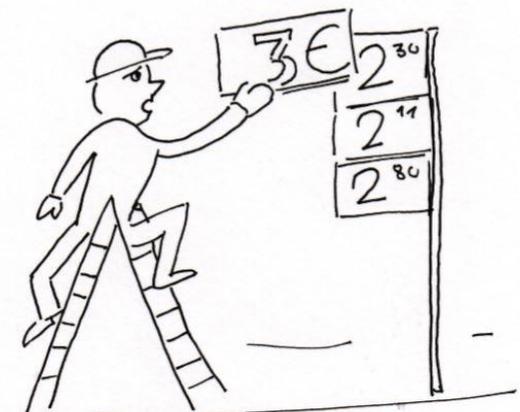
Eine gute Sicherheits-Software kann Sie nicht vor hohen Spritpreisen schützen ...

... aber vor hohen Lösegeldforderungen für Ihre Daten ...

... und vor:

- bösartiger Fremdverschlüsselung
- Datendiebstahl
- Reputationsverlust
- Innentätern
- Schadsoftware
- Unbefugter Anmeldung
- Zugriff via Backdoors

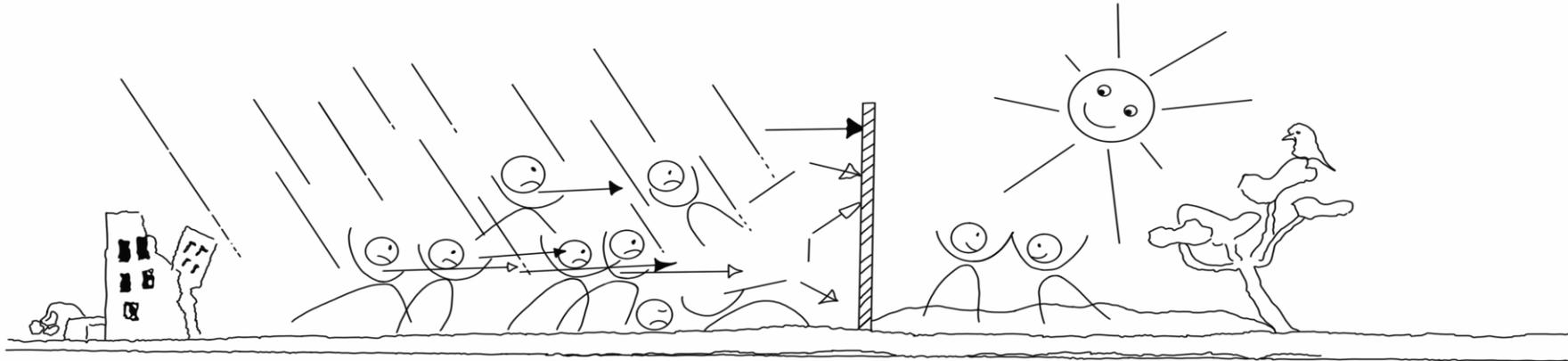
Die neue tetraguard Lösung mit innovativem Denkansatz und bewährten Produktkomponenten wird Sie vor Schäden bewahren, weil Ransomware-Angriffe einfach abprallen



Enjoy Your Security Balance



Vielen Dank für die Aufmerksamkeit



tetraguard systems GmbH
Adolf-Halstrick-Str. 6
53881 Euskirchen
Telefon: +49 2251 81798-0
E-Mail: information@tetraguard.de

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