ERFÜLLEN SIE DIE VORGABEN DER DSGVO?

DER SCHUTZ IHRER DATEN IST WICHTIG

Unterwegs Ihre Daten zu sichern, ist heute eine wichtige Aufgabe – nicht nur für Unternehmen, sondern auch für Privatpersonen.

Was wäre, wenn ein Mitarbeiter Kundendaten auf einer Festplatte mit nach Hause nähme und diese verloren gingen oder gestohlen würden? Oder wenn ein USB-Stick mit Daten über Ihre Bankunterlagen in fremde Hände gelangen würde?

Weltweit gehen jedes Jahr mehr als 2 Millionen dieser kleinen Speichergeräte verloren und Studien haben gezeigt, dass mehr als die Hälfte aller verlorenen USB-Sticks auch tatsächlich verwendet werden.

Ein einfacher Schritt zur Minderung dieses Risikos ist die Nutzung verschlüsselter Geräte. Bei der Verschlüsselung werden die Daten so zerstückelt, dass sie nur jemand mit dem korrekten Code oder Schlüssel lesen kann.

Können Sie es sich leisten, Ihre Daten **nicht** zu verschlüsseln?

Verbatim™

Technology you can trust

WUSSTEN SIE SCHON?

14,717,618,286

DATENSÄTZE WURDEN SEIT 2013 VERLOREN ODER GESTOHLEN

In nur **4 %** dieser Fälle waren die gestohlenen Daten **verschlüsselt** und somit nutzlos für die Diebe waren.

Vom Gesamtanteil der gestohlenen Datensätze verzeichnete **Social Media** den größten Zuwachs bei Sicherheitslücken. Diese stiegen von 1,51 % im Jahr 2017 auf **56,18 %** im Jahr 2018 an. Im selben Zeitraum ging die Anzahl der Lücken und Vorfälle im Gesundheitswesen wesentlich zurück. In der ersten Jahreshälfte 2018 vermeldeten Behörden, Bildungseinrichtungen, Unterhaltungsfirmen, Finanzdienstleister und gemeinnützige Organisationen **50–100 % weniger Sicherheitsvorfälle** als im Jahr davor.

Quelle: Sicherheitslücken-Schwereindex 17.04.2019

DATENSÄTZE WERDEN MIT DER FOLGENDEN HÄUFIGKEIT VERLOREN ODER GESTOHLEN

Jeden Tag	Jede Stunde	Jede Minute	Jede Sekunde
6.404.534	266.856	4.448	74

WAS IST DIE DSGVO?

DSGVO DATENSCHUTZ-GRUNDVERORDNUNG

Die Durchsetzung der DSGVO hat die Vereinheitlichung des Datenschutzrechts auf dem gesamten europäischen Markt erreicht.

Sie hat Unternehmen ein einfacheres und klareres rechtliches Feld gegeben, in dem sie ihren Betrieb führen sollten, und sorgt für mehr Mitspracherecht darüber, was Unternehmen mit ihren Daten machen dürfen.

Für Unternehmen, die die Verordnung nicht einhalten, sind zudem höhere Bußgeldzahlungen vorgesehen. Unternehmen können in Höhe von 4 % des gesamten Jahresumsatzes oder 20 Millionen € bestraft werden.

All dies macht es wichtiger denn je sicherzustellen, dass Ihre kritischen und sensiblen Daten richtig geschützt werden.

MALWARE ERKLÄRT

Viren: Indem diese an Dateien geheftet werden und wiederum andere Dateien infizieren, können sie sich unkontrolliert verbreiten, eine Kernfunktion eines Systems beschädigen und Dateien löschen oder beschädigen.

Rootkits: Software, die es einem Eindringling ermöglicht, sich Root-Zugang zu einem Computersystem zu verschaffen. Sie ist oft versteckt und kann auch Antivirensoftware unbemerkt passieren.

Spyware: Ein Programm, das im Hintergrund verborgen ist, Nutzer ausspäht und ihre Online-Aktivitäten aufzeichnet, darunter Passwörter, Kreditkartennummern, Surf-Verhalten und mehr.

Trojaner: Getarnt als echte Software; Nutzer laden sie in dem Glauben herunter, dass es sich um hilfreiche Software handelt, stattdessen enden sie mit einem infizierten Computer.

Würmer: Das sind selbstreplizierende Programme, die schädliche Codes verbreiten möchten. Sie verwenden Netzwerkschnittstellen und können so ganze Netzwerke infizieren, entweder lokal oder über das Internet.

Ransomware ist eine Art Malware, die Ihre Dateien völlig unbemerkt verschlüsseln und Ihr System unbrauchbar machen kann, worauf dann eine wahllose Online-Zahlung als Gegenleistung für den Entschlüsselungsschlüssel verlangt wird.

AES 256-BIT-VERSCHLÜSSELUNG

WAS IST DIE AES 256-BIT-VERSCHLÜSSELUNG?

AES steht für Advanced Encryption Standard. Das ist eine symmetrische Blockchiffre, die in aller Welt zur Verschlüsselung sensibler Daten eingesetzt wird.

256-Bit gibt die Länge des Schlüssels an, mit dem ein Datenstrom oder eine Datei verschlüsselt wird. Ein Hacker oder Cracker benötigt 2^{256}* verschiedene Kombinationen, um eine mit 256-Bit verschlüsselte Nachricht zu knacken.

AES wurde noch nie geknackt und ist sicher vor jeglichen Brute-Force-Angriffen.

*2^{256} =115.792.089.237.316.195.423.570.985.008.687.907.853.269.984.665.640.564.039.457.584.007.913.129.639.936

FINGERPRINT ACCESS SPEICHERGERÄTE

Nutzt Ihre individuellen biometrischen Daten für volle Informationssicherheit

DURCH FINGERABDRUCK GESCHÜTZTE FESTPLATTE

- Tragbare USB-C™-Festplatte mit eingebautem Fingerabdruck-Scanner
- Zugang über Fingerabdruck von autorisiertem Benutzer
- AES 256-Bit-Hardware-Verschlüsselung
- Bis zu acht autorisierte Fingerabdruck-Benutzer und ein Administrator (über Passwort)
- Sie können vertrauliche Daten speichern und mitnehmen, ohne sich Sorgen um Verlust oder Hackerangriffe zu machen
- USB-C™ zu USB-A-Kabel und USB-C™-Adapter
- Nero Backup-Software inklusive

53650 1 TB | 53651 2 TB

DURCH FINGERABDRUCK GESCHÜTZTER USB-STICK

- Schlanker USB-3.0-Stick aus Aluminium mit eingebautem Fingerabdruck-Scanner
- Zugang über Fingerabdruck von autorisiertem Benutzer
- AES 256-Bit-Hardware-Verschlüsselung
- Bis zu fünf autorisierte Benutzer und ein Administrator
- Sie können vertrauliche Daten speichern und mitnehmen, ohne sich Sorgen um Verlust oder Hackerangriffe zu machen

49337 32 GB | 49338 64 GB | 49339 128 GB

SECURE PRO USB DRIVE

VERSCHLÜSSELTER USB

- 100%-ige Laufwerkverschlüsselung obligatorisch
- Bis zu 12-stelliges Passwort
- 256-Bit AES-Verschlüsselung mit auf einem Sicherheits-Controller basierter Hardware
- Intuitive Autorun-Sicherheitsanwendung vorinstalliert
- Passwort-Hashing-Algorithmus
- Hacker-beständige Passworteingabe – wird nach 10 fehlgeschlagenen Versuchen gelöscht
- Keine Admin-Rechte auf dem Host-PC erforderlich
- Mit PC und Mac kompatibel

98664 16 GB | 98665 32 GB | 98666 64 GB

SPEICHERGERÄTE MIT PIN-CODE-ZUGANG

Erfordert die Eingabe Ihres eigenen Passcodes zum Zugriff auf Daten

SICHERE, TRAGBARE FESTPLATTE MIT INTEGRIERTER TASTATUR

- 100%-ige AES 256-Bit-Hardware-Verschlüsselung
- 5- bis 12-stelliges Passwort
- Nero Backup-Software
- Mit MAC und PC kompatibel
- USB 3.1 Typ-C Gen 1
- Hacker-beständige Passworteingabe – wird nach 20 fehlgeschlagenen Versuchen gelöscht

53401 1 TB | 53403 2 TB

SECURE PORTABLE SSD MIT INTEGRIERTER TASTATUR

- SSDs verwenden Flash-Speicher für höhere Geschwindigkeiten, mehr Leistung und Zuverlässigkeit
- 100%-ige AES 256-Bit-Hardware-Verschlüsselung
- 5- bis 12-stelliges Passwort
- Nero Backup-Software
- Mit MAC und PC kompatibel
- USB 3.1 Typ-C Gen 1
- Hacker-beständige Passworteingabe – wird nach 20 fehlgeschlagenen Versuchen gelöscht

53402 256 GB

SECURE PORTABLE USB-STICK MIT INTEGRIERTER TASTATUR

- Unterstützt die AES 256-Bit-Hardware-Verschlüsselung – alle Daten auf der Festplatte werden nahtlos und in Echtzeit verschlüsselt
- Eingebaute Tastatur für Passworteingabe (bis zu 12 Stellen)
- Kann auch an Fernsehern verwendet werden (mit herkömmlich verschlüsselten Geräten nicht möglich)
- LED-Anzeigen für Strom/Verschlüsselungsstatus
- Mit PC und Mac kompatibel
- Entweder mit USB 3.0 oder USB 3.1 GEN 1 mit USB-C™-Anschluss erhältlich

USB 3.0: 49427 32 GB | 49428 64 GB | 49429 128 GB **USB-C™:** 49430 32 GB | 49431 64 GB | 49432 128 GB

SECURE DESKTOP HDD GEHÄUSE-KIT MIT INTEGRIERTER TASTATUR

- Eingebaute Tastatur für die Passworteingabe
- AES 256-Bit-Hardware-Verschlüsselung
- 3,5“-Festplattengehäuse
- Passt für jede übliche SATA-Festplatte zum Einbau mit 3,5“-Formfaktor
- Einfacher Einbau. Keine umfassenden technischen Fertigkeiten nötig
- USB-C™ auf USB-A-Kabel

53405

BACKUP UND ARCHIVIERUNG

Regelmäßige Datensicherungen schützen sowohl vor versehentlichem als auch vor bösartigem Datenverlust, vor Hardware-Fehlern und Viren bis hin zu menschlichen Fehlern oder Diebstahl, denn die Sicherungen lassen sich zum Wiederherstellen der Original-Datendateien verwenden.

Die Auswahl des richtigen Mediums und Datensicherungsverfahrens ist von vielen Faktoren abhängig:

- Der Menge der zu sichernden Daten
- Dem wahrgenommenen Wert der Daten
- Dem Maß an akzeptiertem Risiko
- Der Dauer, für die Sie die Daten aufbewahren müssen

BEWÄHRTE METHODE VERWENDEN SIE DIE 3-2-1-DATENSICHERUNGSREGEL

3

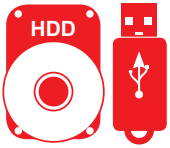
MINDESTENS DREI KOPIEN IHRER DATEN ANLEGEN

Zusätzlich zu Ihren Primärdaten sollten Sie mindestens zwei weitere Sicherungen besitzen, um das Risiko eines Datenverlustes erheblich zu reduzieren. Das könnten physikalische und/oder Cloud-Lösungen sein.

2

DIE KOPIEN AUF MINDESTENS ZWEI UNTERSCHIEDLICHEN MEDIEN SPEICHERN

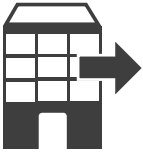
Es ist eine bewährte Praxis, Kopien Ihrer Daten auf mindestens zwei unterschiedlichen Speichertypen zu verwahren, beispielsweise auf internen Festplattenlaufwerken UND auf einem Wechseldatenträger (Bänder, externe Festplatten, USB-Sticks, SD-Karten, CDs, DVDs usw.).



1

MINDESTENS EINE BACKUP-KOPIE EXTERN AUFBEWAHREN

Es ist offensichtlich, aber es ist wirklich keine gute Idee, Ihr externes Speichergerät im selben Raum aufzubewahren wie Ihren Produktionsspeicher.
Ob ein Brand, eine Überschwemmung oder ein Einbruch – Sie würden alle Daten verlieren.



BESTER SCHUTZ VOR ANGRIFFEN - ARCHIVIEREN SIE IHRE DATEN

Um vollständig geschützt zu sein, muss ein Nutzer oder ein Unternehmen die Daten gesichert und offline archiviert haben.

Jedes Gerät, das an ein attackiertes System oder Netzwerk angeschlossen ist, ist gefährdet.

Wenn Ihre Sicherungs-HDD an Ihrem Laptop angeschlossen ist, wenn Ransomware-Software installiert wird, wird auch diese Festplatte verschlüsselt. Die meisten Ihrer Daten auf einem optischen Medium zu archivieren, kann dieses Risiko beseitigen.

OPTISCHE MEDIEN UND LAUFWERKE FÜR DIE ARCHIVIERUNG

- Blu-ray, DVD, CD-Medien – die beste Lösung für eine langfristige Aufbewahrung (25–100 Jahre)
- Verwendung mit den externen DVD- und Blu-ray-Brennern von Verbatim
- Nero Brenn- und Archivierungssoftware, kostenlos zu den Verbatim DVD- und Blu-ray-Brennern

43888 | 43889 | 43890 | 98938 | 43894

RFID-GESCHÜTZTE TASCHEN

SICHERE TASCHEN MIT RFID-GESCHÜTZTEM FACH

- Zum Sortiment gehören Trolleys, Rucksäcke, Kameratasche, Notebook-Taschen, Messenger Bags
- Beinhalten ein spezielles RFID-geschütztes Fach, um das Scannen von Kreditkarten zu verhindern

Paris 49852 | London 49855

ERFÜLLEN SIE DIE VORGABEN DER DSGVO?

Verbatim-Hauptsitz

Verbatim GmbH
Düsseldorfer Str. 13,
65760 Eschborn,
Deutschland
Tel.: +49 (0) 6196 900 10
E-Mail: info.germany@verbatim-europe.com

Verbatim™
Technology you can trust

www.verbatim-europe.com/security