

*Was macht  
Homeoffice zum  
🔥 tinder für  
Cyberkriminelle?*

*It's a Match!*

Homeoffice and Cybercrime have liked each other!



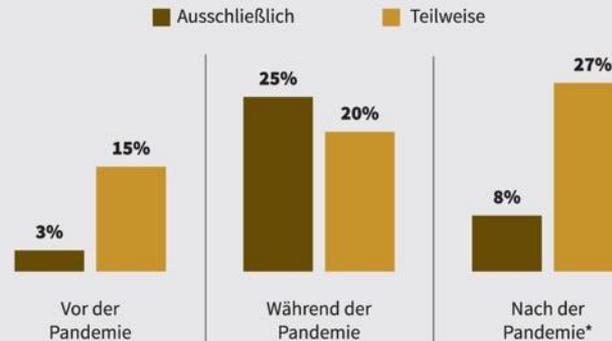
CONTINUE

# THOMAS DEHLER – VORDENKER, PIONIER UND PRAXIS-EXPERTE FÜR REMOTE WORK SEIT 2000



## Corona geht, das Homeoffice bleibt

Anteil der Berufstätigen, die ganz oder teilweise von zu Hause arbeiten



\* voraussichtlich  
Basis: 1503 Erwerbstätige (ab 16 Jahren) in Deutschland; Okt./Nov. 2020  
Quelle: Bitkom



# DAS HOMEOFFICE

## ARBEITSORT MIT ZUKUNFT? MIT SICHERHEIT!

### *Der Kundenservice verlagert sich zunehmend ins Homeoffice*

#### **Gesteigerte Arbeitgeberattraktivität**

- zufriedenerer Mitarbeiter

#### **Größerer Personalmarkt**

- mehr Bewerber

#### **Weniger Präsenzfläche**

- Kosteneinsparung

#### **Mehr Flexibilität**

- Bedarfsorientiertes Arbeiten
- Peak Management

#### **Mehr Sicherheit**

- Business-Kontinuität / Resilienz im Notfall

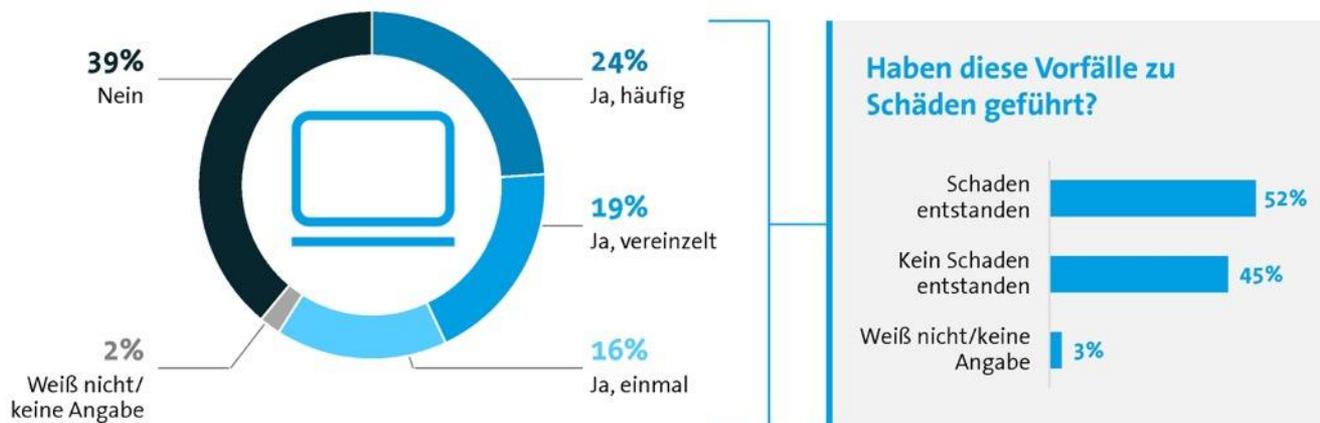


#### **Keine ausdrücklichen gesetzlichen Regelungen in der Datenschutzgrundverordnung (DSGVO) oder im Bundesdatenschutzgesetz (BDSG-neu):**

- Arbeitgeber ist datenschutzrechtlich Verantwortlicher im Sinne der DSGVO
- Arbeitgeber ist verpflichtet, für die Einhaltung des Datenschutzes zu sorgen
- Grundsätzlich gilt: Im Homeoffice gelten die selben Anforderungen an den Datenschutz wie im Büro!
- Besondere Gefahren für die Datensicherheit:
  - *Weniger Überwachungsmöglichkeiten des Arbeitgebers;*
  - *Ggf. fehlende IT-Infrastruktur;*
  - *kein Einfluss darauf, welche „betriebsfremden“ Personen Zugang haben*

### Homeoffice als weiteres Einfallstor im Pandemiejahr

Hat es seit Beginn der Corona-Pandemie IT-Sicherheitsvorfälle in Ihrem Unternehmen gegeben, die auf die Arbeit im Homeoffice zurückzuführen sind?



Basis links: Alle befragten Unternehmen, bei denen Homeoffice generell möglich ist (n=817); Basis rechts: Alle befragten Unternehmen, bei denen es seit Beginn der Corona-Pandemie IT-Sicherheitsvorfälle gab, die auf die Arbeit im Homeoffice zurückzuführen sind (n=483) | Quelle: Bitkom Research 2021

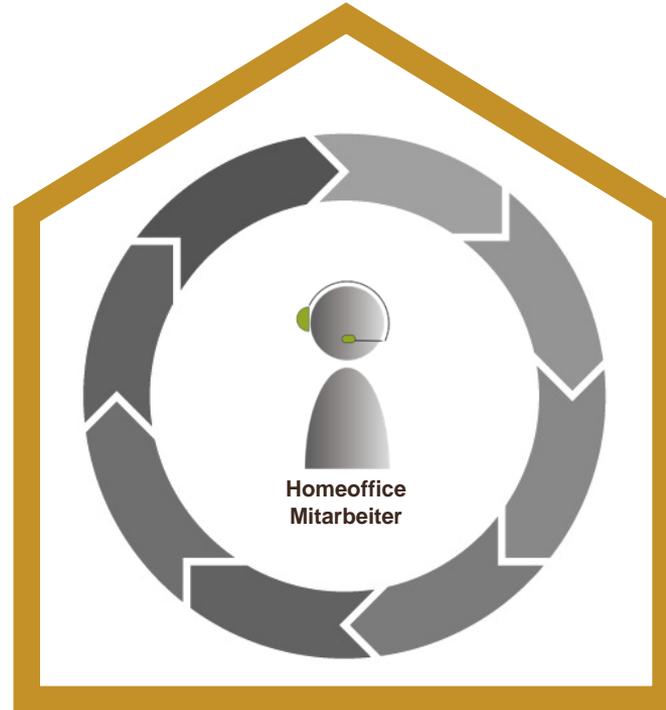
bitkom

# NEW NORMAL - DISTANZ-ARBEIT

## ORT ALS ERWEITERTER FOKUS

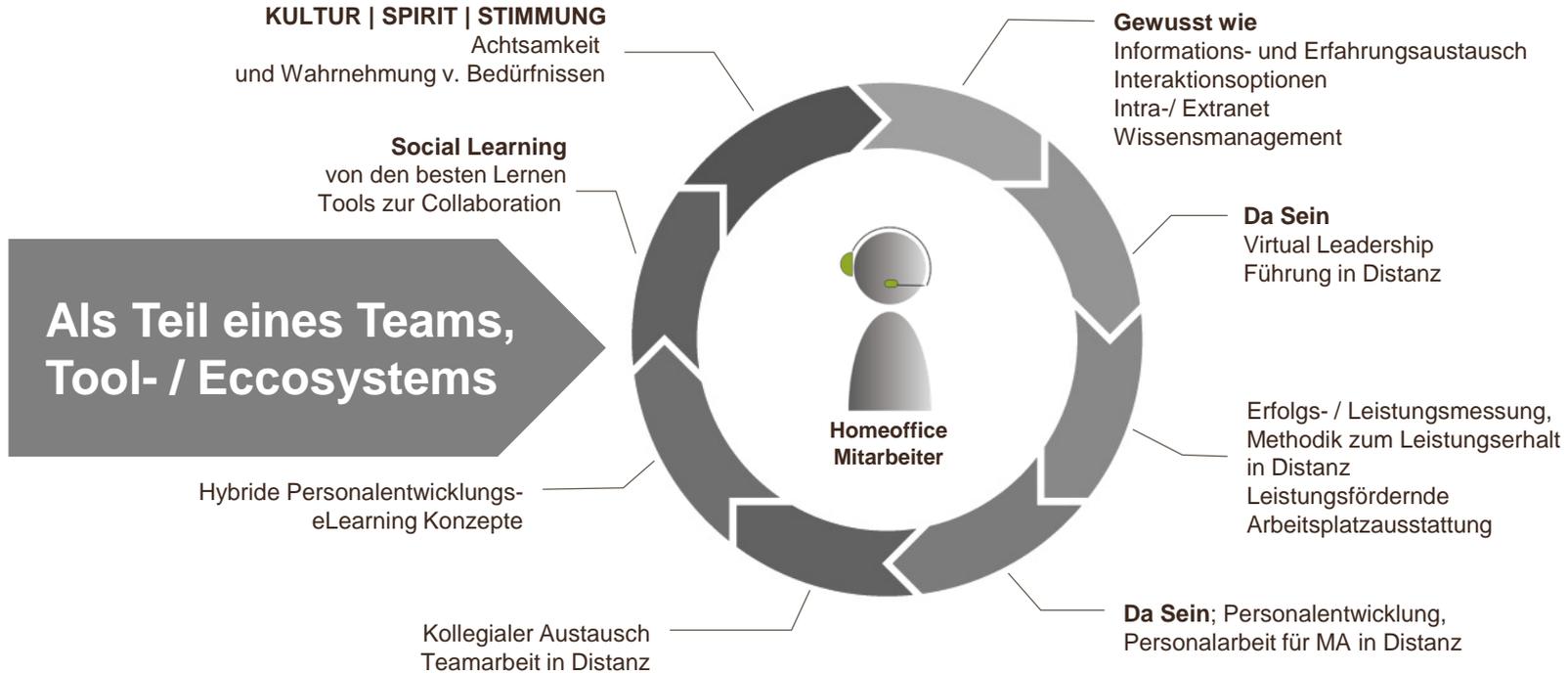
### An einem Ort:

- a. Privat
- b. Öffentlich
- c. Unternehmen

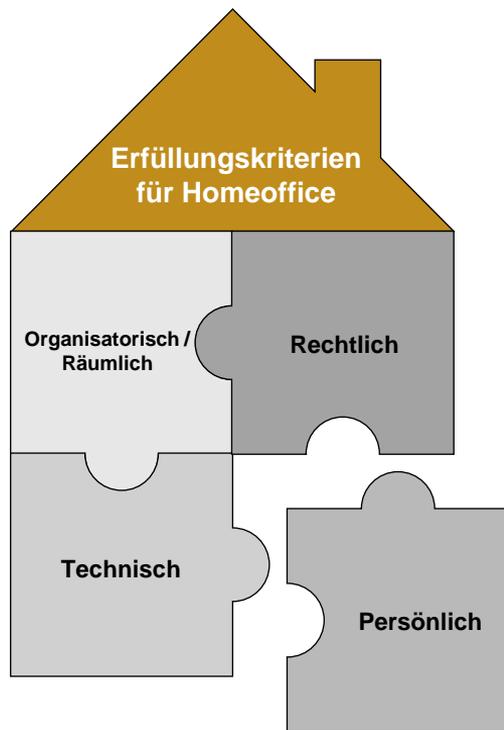


# NEW NORMAL - DISTANZ-ARBEIT

## ORT ALS ERWEITERTER FOKUS



# ORGANISATORISCHE RAHMENBEDINGUNGEN UND MITWIRKUNGSPFLICHTEN DES BESCHÄFTIGTEN FÜR HOMEOFFICE



## Organisatorische / Räumliche Kriterien

- ArbStättV
- Zugangs- und Zutrittsmöglichkeiten
- BetrVG
  - Ergonomische Ansprüche an Arbeitsgerät und Arbeitsplatz
  - Ansprüche an Raum (z.B. Blendschutz, Lärm, Belüftung)

## Rechtliche Kriterien

- DSGVO | ArbMedVV | DGUV
- Prüfung und Aktualisierung der Gefährdungsbeurteilung nach §§ 5 und 6 ArbSchG;
- Garantierte Unverletzlichkeit der Wohnung

## Technische Kriterien

- BSI
- IT-Grundschutz und IT-Sicherheit
- Anbindung Breitbandnetz

## Informationswissen

Mehr unter:  
[gefta.eu/checklisten](https://gefta.eu/checklisten)

## RÄUMLICHE ANFORDERUNGEN (EXEMPLARISCHER AUSZUG)

Ist die Wohnung des Mitarbeiters ausreichend groß, um einen Distanzarbeitsplatz einzurichten (eigener Raum oder Raumteil)?	✓
Kann in dem für HO vorgesehenen Raum ein ergonomischer Arbeitsplatz eingerichtet werden, welcher die nachstehenden Kriterien erfüllt?	✓
Charakter eines Arbeitszimmers/Wohnraumes (z.B. kein Kellerraum)	✓
keine Mitbenutzung des Raumes / Raumteils durch Mitbewohner während der Arbeitszeit	✓
Vertraulichkeit des Raumes gewährleistet	✓
Sichtverbindung nach draußen / natürliche Belüftung (Fenster)	✓
ausreichend große Bewegungsfläche (mind. 8 qm)	✓
ergonomische Beleuchtung & ausreichend großer Arbeitstisch / Beinfreiheit	✓
ergonomischer Bürodrehstuhl	✓
ergonomische Aufstellung der Arbeitsmittel möglich (Bildschirm, Tastatur, Telefon etc.)	✓

### Informationswissen

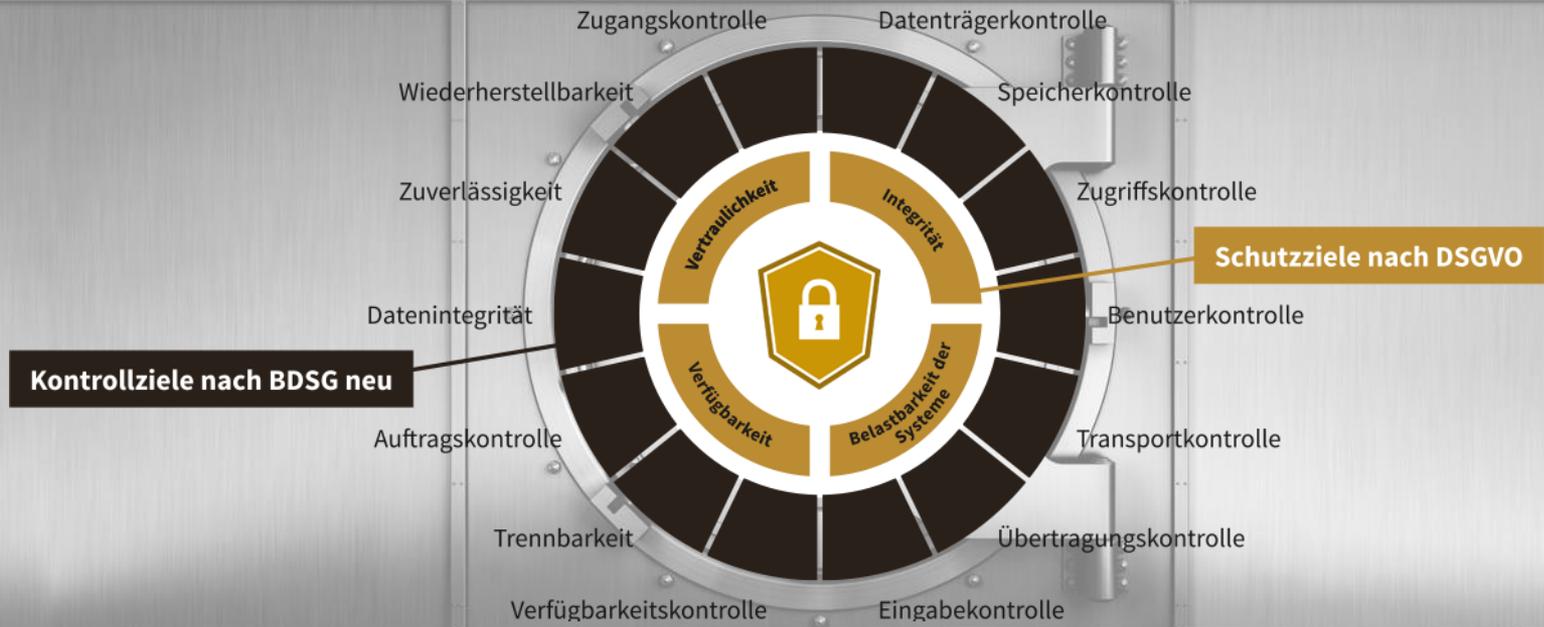
Mehr unter:  
[gefta.eu/checklisten](https://gefta.eu/checklisten)

## Insbesondere:

- Generelle **IT-Schutzmaßnahmen** (Firewall, Anti-Viren-Programm, etc.)
- Sicherer **Remote-Zugriff** auf Unternehmensnetzwerk (insb. VPN)
- **Verschlüsselung** der elektronischen Kommunikation
- **Vermeidung** lokaler Datenspeicherung
- Vorkehrungen zum Umgang mit dem Verlust mobiler Endgeräte

*Anforderungen sind höher, je sensibler und schützenswerter die Daten!*

# DSGVO FORDERT DIE SICHERSTELLUNG DER VIER SCHUTZZIELE – AUCH IM HOMEOFFICE GLEICHZEITIG EMPFIEHLT SICH DIE EINHALTUNG DER KONTROLLZIELE



## *Typische Herausforderungen im Homeoffice*

### **Device-Management**

Sowohl Geschäftsrechner als auch privater PC müssen den sicheren Datenzugriff ermöglichen.

### **Nutzer-Authentisierung**

Das Authentifikations-Verfahren zur Identitätsfeststellung des Nutzers muss verlässlich sein.

### **Datenschutz Compliance**

Das Unternehmen muss für DSGVO-konforme Strukturen und Prozesse sorgen.

### **Internetverbindung**

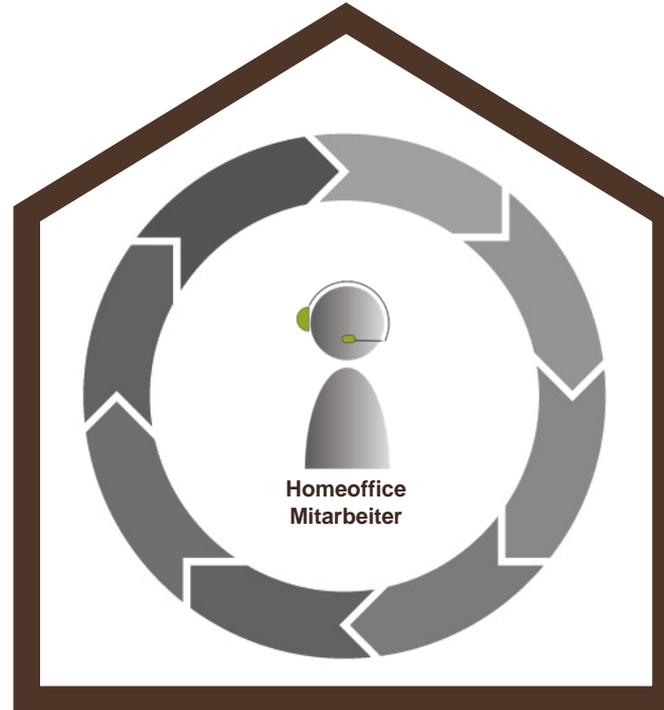
Das Unternehmen muss sicherstellen, dass die Internetverbindung sicher ist.

# NEW NORMAL - DISTANZ-ARBEIT

## ORT ALS ERWEITERTER FOKUS

### An einem Ort:

- a. Privat
- b. Öffentlich
- c. Unternehmen



Mit der technischen Verbindung VPN in die Cloud und die digitale Arbeitswelt verbunden.

**VPN**

**CONNECTION / VERBINDUNG  
IM CYBERCRIMEFOKUS plus  
IDENTITÄTSKLAU /  
- MANIPULATION**

**Wer ist der Nutzer  
am Zugangspunkt?**



*Das BSI empfiehlt  
die sichere  
Dreifaltigkeit aus:  
**MFA | VPN | DM***

### Nutzer-Authentisierung

Eine Nutzer-Authentisierung sollte mit einer sicheren Mehr-Faktoren-Authentisierung (MFA) erfolgen, bestenfalls mittels Video-Ident-Verfahren.

### VPN

Die VPN-Autorisierung sollte dezentral erfolgen, sodass das VPN nicht kompromittiert werden kann.

### Device-Management

Es empfiehlt sich eine verschlüsselte Desktop-Umgebung, die geschäftliche Daten von privaten trennt. So lassen sich Privat-PC, COPE, CYOD sicher und DSGVO-konform im Homeoffice nutzen.



## *Kundendaten sind ein beliebtes Ziel für Cyberattacken und Datendiebstahl*

**Jedes dritte Unternehmen** musste während der Pandemie aktiv auf Cyberangriffe im Homeoffice reagieren, von den Großunternehmen sogar jedes vierte.

Das ist nur die Spitze des Eisbergs. Die meisten Cyberangriffe und Datendiebstähle bleiben unentdeckt.

# BEISPIEL EINER SOCIAL REENGINEERING AKTION

## ABSENDERADRESSE BEACHTEN

Von: Sparkasse <kudnenservice@sparkasse.de>  
Gesendet: Mittwoch, 17. November 2021 13:34  
An: Thomas Dehler <tdehler@value5.com>  
Betreff: Wichtiger Hinweis zu Ihrem Konto



Von: Sparkasse <kudnenservice@sparkasse.de> !!!  
Gesendet: Mittwoch, 17. November 2021 13:34  
An: Thomas Dehler <tdehler@value5.com>  
Betreff: Wichtiger Hinweis zu Ihrem Konto

 Sparkasse  
Langen-Seligenstadt

## Wir ändern unsere Verfahren

### Wichtige Mitteilung

#### Sehr geehrter Kunde,

Wir müssen Sie darüber in Kenntnis setzen, dass wir zeitnah ein neues Sicherheitsverfahren für unsere Kunden implementieren werden. Durch unser neues, ausgeprägtes Sicherheitsverfahren namens S-CERT, werden Ihre vertraulichen Daten noch besser verschlüsselt und sind somit noch mehr gesichert.

**Durch eine neue Datenschutzreform müssen wir jeden Kunden auf unser neues System hinweisen.**

Damit Sie sich mit unserem neuen System vertraut machen, bitten wir alle unsere Kunden, sich über den nachfolgenden Link über die Neuerungen zu informieren. Loggen Sie sich bequem über den Button ein:

[Zum Verfahren](#)

Wir bitten um Verständnis für die Situation

Mit freundlichem Gruß  
Ihre Sparkasse

2021- Sparkasse

# ANGEBOT IM DARK-NET

## CYBERCRIME IST „LEICHT UND GÜNSTIG“ KÄUFLICH

### Welcome to the Dark Web Hackers

Have you tried to buy hacking services on the dark web before? Not happy with the results? Only empty promises but no one getting the job done?

Then you should try Vladimir and George, the dark webs most trusted hackers for getting things done.

Unlike others, our prices are not the cheapest, but if we can't do a job, you will get a full refund!

#### Vladimir



Hello, my name is Vladimir.  
I am the technical expert at dark web hackers.

My expertise is programming, running exploits, setting up DDOS attacks and i like the challenge of doing things where most others give up. I can "recover" passwords of most social networks easily, remote control smartphones, and most other things that are useful because i spent years to find methods that really work.  
Here you can find a list of my services, if it is not listed, then minimum price will be \$600 and we will discuss the final price once you gave me all information and i accept the job.

Product	Price	Quantity
Remote control the phone of someone else, most new models supported	700 USD = 0.01166 ₿	1 X <a href="#">Buy now</a>
Facebook and Twitter account hacking	500 USD = 0.00833 ₿	1 X <a href="#">Buy now</a>
Other social network account hacks, for example reddit or instagram	450 USD = 0.00750 ₿	1 X <a href="#">Buy now</a>
Full package deal, getting access to personal or company devices and accounts and searching for the data you need.	1800 USD = 0.02998 ₿	1 X <a href="#">Buy now</a>
DDOS for protected websites for 1 month	900 USD = 0.01499 ₿	1 X <a href="#">Buy now</a>
DDOS for unprotected websites for 1 month	400 USD = 0.00666 ₿	1 X <a href="#">Buy now</a>
Hacking webservers, game servers or other internet infrastructure	1300 USD = 0.02166 ₿	1 X <a href="#">Buy now</a>

#### George



Hello, my name is George.  
My hacking skills are not as perfect as Vladimir's, but i am really good with social engineering. And i really like messing with people, i don't care what you want to do to them.  
If there is something i can't do then Vladimir will help and teach me for next time.

Product	Price	Quantity
Destroying someone's life: Your target will have legal problems or financial problems, proven methods including child porn that always works	1700 USD = 0.02832 ₿	1 X <a href="#">Buy now</a>
Spreading false information about someone on social media, not as life ruining but still nasty	450 USD = 0.00750 ₿	1 X <a href="#">Buy now</a>
Social engineering to get secrets from a person, private or from some employee	450 USD = 0.00750 ₿	1 X <a href="#">Buy now</a>
Other social engineering work	500 USD = 0.00833 ₿	1 X <a href="#">Buy now</a>
30 days full service, i will work 8 hours per day for 30 days only on your project	7500 USD = 0.12494 ₿	1 X <a href="#">Buy now</a>
Only additionally: priority service or 1 full day extra work for complicated cases	400 USD = 0.00666 ₿	1 X <a href="#">Buy now</a>
Only additionally: Add this item if your target is a high profile VIP or large public company	2500 USD = 0.04165 ₿	1 X <a href="#">Buy now</a>

# ANGEBOT IM DARK-NET

## CYBERCRIME IST „LEICHT UND GÜNSTIG“ KÄUFLICH

### Cardshop

[Products](#) [Register](#) [Login](#)

#### USA CVV KNOWN BALANCE



You will get a High Quality known balance cc (100% live not some rubbish cards like my competitor ones) !  
You will get the current balance (how much is owed to bank by CH ) You will get available credit (so you know exactly how much to charge !  
You will also get last statement date /amount and next statement due /amount just so you get your head round it (in case your method takes a while you know exactly how to move around it.

You will receive the following card format:  
CC number | expiry | CVV | first name | last name | address | city | State | zipcode | email | phone number (where available) | current balance | available credit |

Cards designed for Paypal/stripe/square/venmo no more wasting time and money trying to find a card that works, with me you will hit first time guaranteed!

Always bought cards not knowing how much to charge, and worried about charging too much and killing the card? NOT with my cards, you will know EXACTLY how much is in there so you can charge it without worrying !  
Happy buying !

Product	Price	Quantity
10 x cards with credit from 1000 to 5000 USD	90 USD = 0.00150 B	<b>Sold out</b>
50 x cards with credit from 1000 to 5000 USD	350 USD = 0.00583 B	1 X <a href="#">Buy now</a>
10 x cards with credit from 5000 to 20000 USD	120 USD = 0.00200 B	1 X <a href="#">Buy now</a>
50 x cards with credit from 5000 to 20000 USD	450 USD = 0.00750 B	1 X <a href="#">Buy now</a>
10 x cards with credit from 20000 to 50000 USD	180 USD = 0.00300 B	1 X <a href="#">Buy now</a>
50 x cards with credit from 20000 to 50000 USD	650 USD = 0.01083 B	1 X <a href="#">Buy now</a>
10 x non verified by visa cards 5000 - 100000 USD	250 USD = 0.00416 B	1 X <a href="#">Buy now</a>

### Schäden steigen auf 223 Mrd. Euro: Erpressung und Systemausfälle als treibende Faktoren (+358% ggü. 2019)

Wodurch sind Ihrem Unternehmen innerhalb der letzten 12 Monate Schäden im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2021)	Schadenssummen in Mrd. Euro (2019)	Schadenssummen in Mrd. Euro (2017)	Schadenssummen in Mrd. Euro (2015)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	61,9	13,5	5,3	7,2
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	24,3	5,3	0,7	1,5
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	17,1	4,4	3,2	2,0
Patentrechtsverletzungen (auch schon vor der Anmeldung)	30,5	14,3	7,7	9,4
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	29,0	11,1	8,6	6,4
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	22,7	11,1	3,5	11,5
Imageschaden bei Kunden oder Lieferanten/Negative Medienberichterstattung	12,3	9,3	7,7	5,9
Kosten für Ermittlungen und Ersatzmaßnahmen	13,3	18,3	10,6	-
Kosten für Rechtsstreitigkeiten	12,4	15,6	5,5	6,5
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	-	-	2,2	0,9
Sonstige Schäden	0	<0,1	<0,1	0,1
<b>Gesamtschaden pro Jahr</b>	<b>223,5</b>	<b>102,9</b>	<b>54,8</b>	<b>51,2</b>

Basis: Selbsteinschätzung aller befragten Unternehmen, die in den letzten 12 Monaten (vor 2021: in den letzten 2 Jahren) von Diebstahl, Industriespionage oder Sabotage betroffen waren (2021: n=935; 2019: n=801; 2017: n=571; 2015: n=550) | Quelle: Bitkom Research 2021

bitkom

# CHECKLISTE -AUSZUG

## DATENSCHUTZ UND IT-SICHERHEIT IM HOMEOFFICE

Werden unter Berücksichtigung der Besonderheiten des Arbeitens im Homeoffice geeignete organisatorische und technische Maßnahmen ergriffen, um die Sicherheit der Daten zu gewährleisten?	✓
Besteht eine auf die betrieblichen Belange und Realitäten zutreffende Vereinbarung (Homeoffice Policy) zwischen Arbeitgeber und Beschäftigten zur Arbeit im Homeoffice?	✓
Können oder müssen die Mitarbeiter auf eigene Geräte zurückgreifen und gibt es dazu eine Nutzungsvereinbarung (BYOD)?	✓
Falls Privatgeräte verwendet werden müssen: Werden betriebliche und private Daten getrennt?	✓
Existiert ein Berechtigungssystem, um zu gewährleisten, dass Beschäftigte nur auf die für ihre Arbeit erforderlichen Bereiche Zugriff haben?	✓
Sind die verwendeten Geräte technisch auf dem aktuellsten Stand und werden laufend aktualisiert? Sind Virens Scanner und Firewalls aktiv?	✓
Ist die Nutzung der betrieblichen Endgeräte zu privaten Zwecken sowie der Einsatz von privaten USB-Speichern untersagt oder anderweitig geregelt?	✓

### Informationswissen

Mehr unter:  
[gefta.eu/checklisten](https://gefta.eu/checklisten)

# ERFAHRUNGEN WARUM IT SICHERHEIT & DATENSCHUTZ IM HO LÜCKEN AUFWEISEN

- 1. Gefühle werden ausgeblendet**
2. Keine ausreichende Kapazität
3. Keine ausreichende Kompetenz
4. Notwendigkeit ist nicht verstanden / wird ausgeblendet
5. Haltung
- 6. Verantwortungsfurcht, - flucht**
7. Untergang in Komplexität
- 8. FK glauben, wiegen sich in falscher Sicherheit**
9. Mangel an schnellen, einfachen Verfahren
10. Regelsysteme wurden nicht geändert
11. Scham, Scheu an Defiziten zu arbeiten / arbeiten zu lassen
12. Zu viel gestern, zu viel morgen
13. Scheu vor politischer Dimension
14. Fehlende Sensibilität
- 15. Generelle Defizite in Kultur, Zusammenarbeit, Verantwortungs- und Handlungsbewußtsein**
16. Scheu und kurzsichtige, Risikoanalyse

# SICHERES DEVICE / DESKTOP MANAGEMENT

## PROTOKOLL ALLER ERFOLGTEN AUTORISIERUNGEN (Zugriffsort, Mitarbeiter, Device)

Secure Desktop Management

Autorisierungs Protokoll

Suche

Partnername	Name Agent	Verbindung Agent	Name Concierge	Verbindung Agent	Trennung	Aktion	Mitteilung / Grund	Notiz
Partnername	Name des Beschäftigten	Zeitpunkt der Anfrage	Name des eConcierges	Zeitpunkt der Verbindung	Zeitpunkt der Trennung	Resultat der Autorisierung	Anmerkung zur Autorisierung	Optionale Notizen

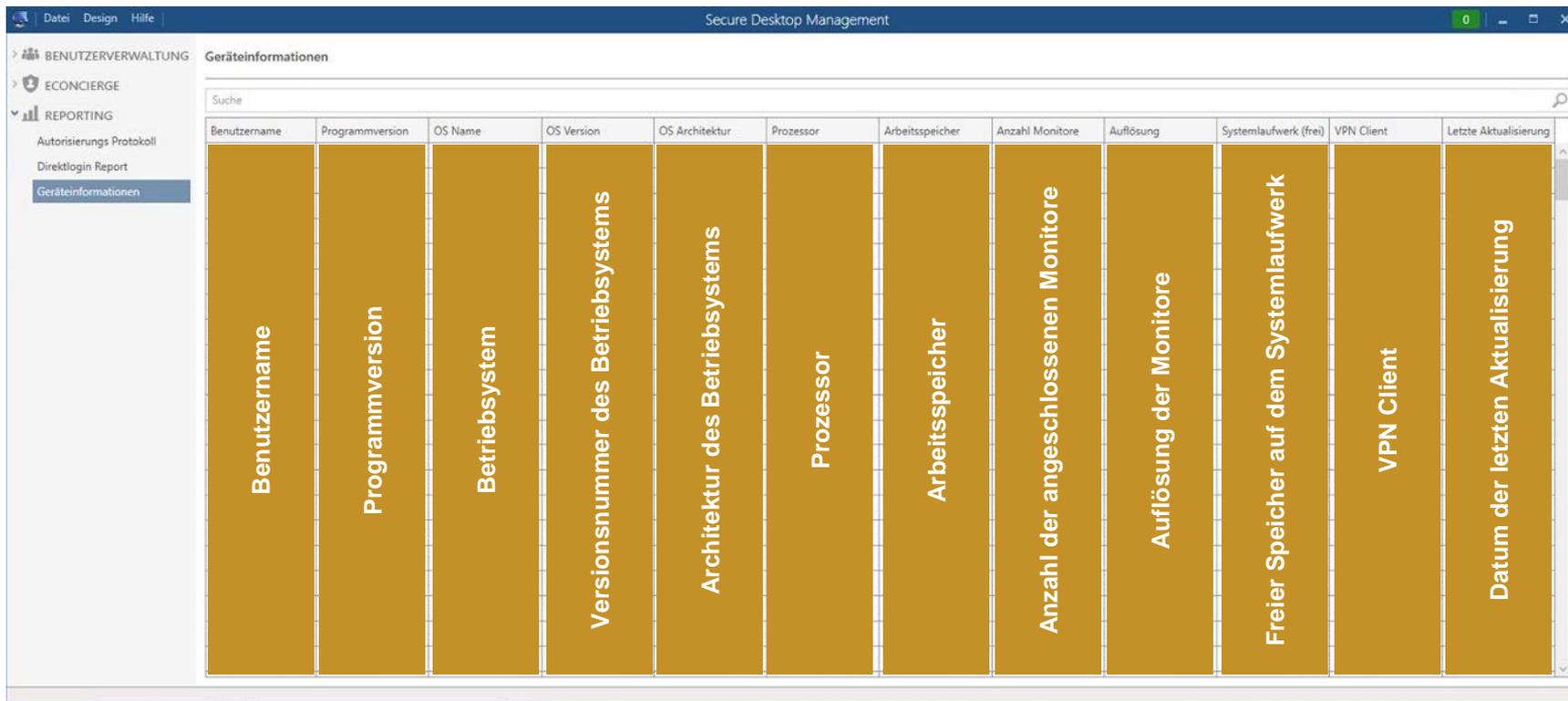
Zeitraum von 16.06.2021 00:00:00

Zeitraum bis 17.06.2021 00:00:00

AKTUALISIEREN

# SICHERES DESKTOP / DEVICE MANAGEMENT

## ÜBERSICHT DER ERFASSTEN GERÄTEINFORMATIONEN



The screenshot shows the 'Geräteinformationen' (Device Information) section of the 'Secure Desktop Management' application. The interface includes a sidebar with navigation options like 'BENUTZERVERWALTUNG', 'ECONCIERGE', and 'REPORTING'. The main area displays a table with 12 columns, each containing a label for a specific device attribute. The labels are: Benutzername, Programmversion, Betriebssystem, Versionsnummer des Betriebssystems, Architektur des Betriebssystems, Prozessor, Arbeitsspeicher, Anzahl der angeschlossenen Monitore, Auflösung der Monitore, Freier Speicher auf dem Systemlaufwerk, VPN Client, and Datum der letzten Aktualisierung.

Benutzername	Programmversion	OS Name	OS Version	OS Architektur	Prozessor	Arbeitsspeicher	Anzahl Monitore	Auflösung	Systemlaufwerk (frei)	VPN Client	Letzte Aktualisierung
Benutzername	Programmversion	Betriebssystem	Versionsnummer des Betriebssystems	Architektur des Betriebssystems	Prozessor	Arbeitsspeicher	Anzahl der angeschlossenen Monitore	Auflösung der Monitore	Freier Speicher auf dem Systemlaufwerk	VPN Client	Datum der letzten Aktualisierung

# GESICHERTE KENNTNISSE DER ARBEITSORTE ÜBERSICHT UND VERWALTUNG DER HINTERLEGTEN UND AUDITIERTEN VERTRAUENSARBEITSORTE (REFERENZBILDER DER BEGEHUNG)

The screenshot displays the 'Secure Desktop Management' application window. The title bar includes 'Datei', 'Design', 'Hilfe', and 'Secure Desktop Management'. The left sidebar contains a navigation menu with 'BENUTZERVERWALTUNG' (selected), 'ECONCIERGE', 'Autorisierung', 'Bildverwaltung', and 'REPORTING'. The main area is titled 'Bildverwaltung' and features a search bar labeled 'Suche'. Below the search bar is a table with three columns: 'Benutzername', 'Vorname', and 'Nachname'. The table cells are currently empty, showing only the column headers. To the right of the table is a large orange box with the text 'Hinterlegte Referenzbilder' and three small numbered buttons (1, 2, 3) below it. At the bottom right of the interface are buttons for 'ÄNDERN', 'LÖSCHEN', and 'ABBRECHEN'.

Benutzername	Vorname	Nachname

# SECURE DESKTOP MANAGEMENT

## AUTORISIERUNGSPROZESS | ANSICHT LIVE ZUTRITTSKONTROLLE

The screenshot displays the 'Secure Desktop Management' application window. The title bar includes 'Datei', 'Design', 'Hilfe', and 'Secure Desktop Management'. The left sidebar contains a navigation menu with the following items: 'BENUTZERVERWALTUNG', 'ECONCIERGE' (expanded), 'Autorisierung' (selected), 'Bildverwaltung', 'MODULVERWALTUNG', 'PARTNERVERWALTUNG', 'PROFILVERWALTUNG', 'REPORTING', and 'SINGLE SIGN ON'. The main content area is titled 'Autorisierung' and features a 2x4 grid of orange panels. The top row panels are: 'Warte-schlange der Anfragen zur Autorisierung', 'Live-Video des Beschäftigten mit Zutrittsanfrage bei Arbeitsantritt' (with subtext 'Erlauben / Verbieten'), 'Referenzbild zum Abgleich aus Raumbegehung' (with subtext '3 Bildoptionen oder Neu'), and 'Live-Bild des eConcierges' (with subtext 'Rolle als Supervisor, Sekretariat, Teamleiter, IT-Helpdesk'). The bottom row panels are: 'Liste der aktiven eConcierges', 'Informationen zum aktuell anfragenden Beschäftigten', 'Optionale, interne Notizen zum aktuell anfragenden Beschäftigten', and 'Notizen aus der Historie zum aktuell anfragenden Beschäftigten'. An 'AUSLOGGEN' button is located in the bottom right corner of the interface.

Panel 1	Panel 2	Panel 3	Panel 4
Warte-schlange der Anfragen zur Autorisierung	Live-Video des Beschäftigten mit Zutrittsanfrage bei Arbeitsantritt Erlauben / Verbieten	Referenzbild zum Abgleich aus Raumbegehung 3 Bildoptionen oder Neu	Live-Bild des eConcierges Rolle als Supervisor, Sekretariat, Teamleiter, IT-Helpdesk
Liste der aktiven eConcierges	Informationen zum aktuell anfragenden Beschäftigten	Optionale, interne Notizen zum aktuell anfragenden Beschäftigten	Notizen aus der Historie zum aktuell anfragenden Beschäftigten

# HOMEOFFICE IST UND BLEIBT MIT SICHERHEIT CHEFSACHE

## WANN SPRECHEN WIR PERSÖNLICH?

### LinkedIn

[linkedin.com/in/thomas-dehler-59a0a89](https://www.linkedin.com/in/thomas-dehler-59a0a89)

### Xing

[xing.com/profile/Thomas\\_Deidler](https://www.xing.com/profile/Thomas_Deidler)

### Twitter

[twitter.com/Thomas\\_Deidler](https://twitter.com/Thomas_Deidler)

### Kostenloses Erstgespräch

[is.gd/xnGGpP](https://is.gd/xnGGpP)



# HOMEOFFICE MIT SICHERHEIT IST / BLEIBT CHEFSACHE

UNSERE PASSION FÜR IHREN WEG ZUM PERFEKTEN REMOTE WORK KONZEPT

## TSD Demo

Wir präsentieren Ihnen kostenlos und unverbindlich in 20-30 Minuten Highlights des TSD und beantworten Ihre individuellen Fragen.



[is.gd/mp3xz5](https://is.gd/mp3xz5)

## GEFTA Portfolio

Entdecken Sie unser gesamtes Angebot an Lösungen zur Arbeitsortflexibilisierung und zu Remote Work Arbeitsmodellen.



[gefta.eu/services](https://gefta.eu/services)

© GEFTA | Gesellschaft für Telearbeit mbH

**2021**

**Die Inhalte sind nicht zur Veröffentlichung, Weitergabe  
oder Verwertung freigegeben.**