



Der richtige Schutz  
vor den  
unsichtbaren Gefahren

**Cyber Versicherung für  
Firmen & freie Berufe**

Torsten Krüger | Hannover | 04.02.2020



# Agenda

- > 1 HDI stellt sich vor
  - Ihre Ansprechpartner
- 2 Ausgangs- und Bedrohungslage
- 3 Das Cyber-Security-Konzept
- 4 Kosten / Prämien / Berechnung
- 5 Fragen
- 6 Fazit

herzlich willkommen  
im Namen von...



# HDI - ein starker Partner an Ihrer Seite

## Versicherungsverein auf Gegenseitigkeit

1903

über **100 Jahre** Erfahrung im Versicherungsgeschäft



2020

1	<ul style="list-style-type: none"><li>Die Nummer 1 im deutschen Markt bei Steuerberatern und niedergelassenen Ärzten</li></ul>
2	<ul style="list-style-type: none"><li>Platz 2 bei Wirtschaftsprüfern</li></ul>
3	<ul style="list-style-type: none"><li>Drittgrößte deutsche Versicherungsgruppe</li><li>Platz 3 bei Architekten, Ingenieuren und Sachverständigen</li></ul>

# Ihr Ansprechpartner für das Sach-Geschäft



# Agenda

- 1 HDI stellt sich vor
  - Ihre Ansprechpartner
- > 2 Ausgangs- und Bedrohungslage
- 3 Das Cyber-Security-Konzept
- 4 Kosten / Prämien
- 5 Fragen
- 6 Fazit

# die unsichtbaren Gefahren



kurz gesagt...



Es gibt zwei Arten von Unternehmen:  
Solche, die schon gehackt wurden, und  
solche, die es noch werden.“



Robert Mueller, Ex-Direktor des FBI (2001-2013)



Kurz gesagt...!?



- ◉ Gezielter Angriff
- ◉ Gestreuter Angriff
- ◉ Sabotage (Innenangriff)

# mich betrifft das nicht...!?

## Presse aus den letzten Wochen

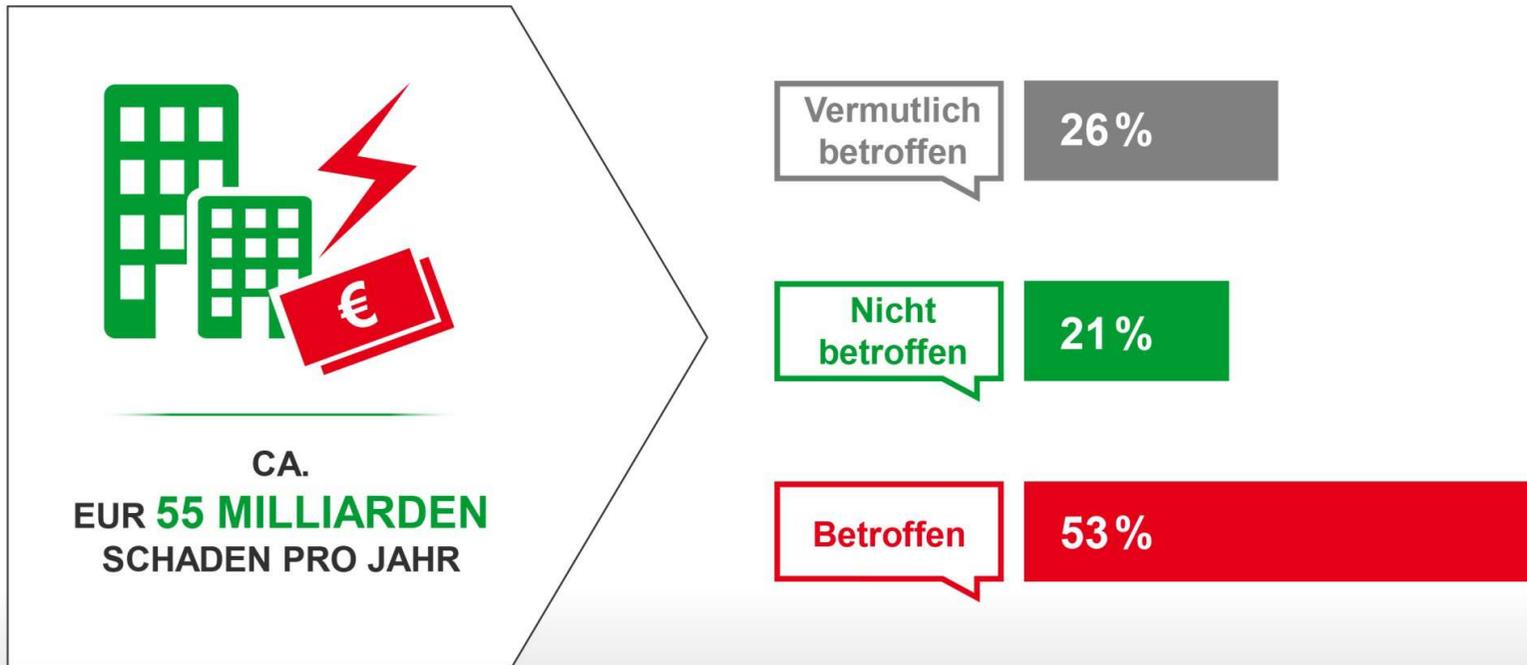
The screenshot shows a social media interface with several recommendation cards. The main card is from Torsten Krüger, dated 9. Dez 2018, 20:14. It features a photo of a person's hands holding a credit card with a glowing green triangle on it. The headline is "Taschendiebstahl 2.0: So einfach ist der Datenklau über Funk-Chips". The text below reads: "Die neuen Kreditkarten sind praktisch. Man muss sie gar nicht erst aus der Geldbörse kramen – auflegen genügt. Andererseits sind sie gefährlich. Denn die NFC-Chips auf der Kreditkarte machen es...". Below the text is a link to "Pfefferminzia - Das Multimedia für Versicherungsprofis". To the right of the main card, there is a partial view of another article with the headline "on Millionen VE - Netzwelt" and the text "g. Nun kam heraus: ütz in der Cloud". At the bottom right of the main card, there is a small text "abgelegt. SPIEGEL ONLINE". The interface includes profile pictures, names, dates, and interaction icons (like, comment, share).



Mich betrifft das nicht...!?

Ca. 80% der Unternehmen sind (vermutlich) betroffen kompetent

Anteil der deutschen Unternehmen, die in den letzten zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren



Quelle: Wirtschaftsschutz in der digitalen Welt, Bitkom Juli 2017

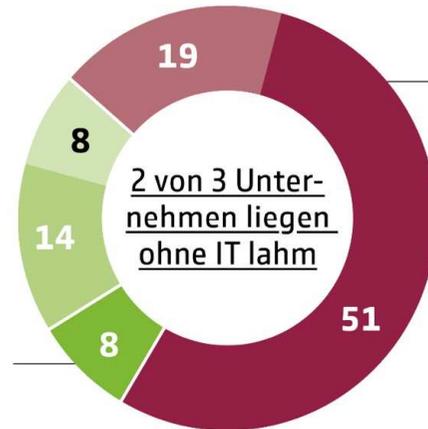
## Mich betrifft das nicht...!?

### Eine nicht funktionierende Unternehmens-IT legt schnell auch die meisten Betriebe lahm

Würde die IT mehrere Tage ausfallen, wäre ihr Betrieb ...  
(Angaben in Prozent)

- nicht eingeschränkt
- nur wenig eingeschränkt
- nicht so stark eingeschränkt
- eher stark eingeschränkt
- sehr stark eingeschränkt

**Nur 8 %** geben an, dass Ihr Unternehmen ohne IT gar nicht eingeschränkt wäre.



# 70%

wären ohne funktionierende Unternehmens-IT eher oder sehr stark eingeschränkt.

### Freiberufler sind gegenüber anderen Unternehmern in besonderem Maße haftbar!

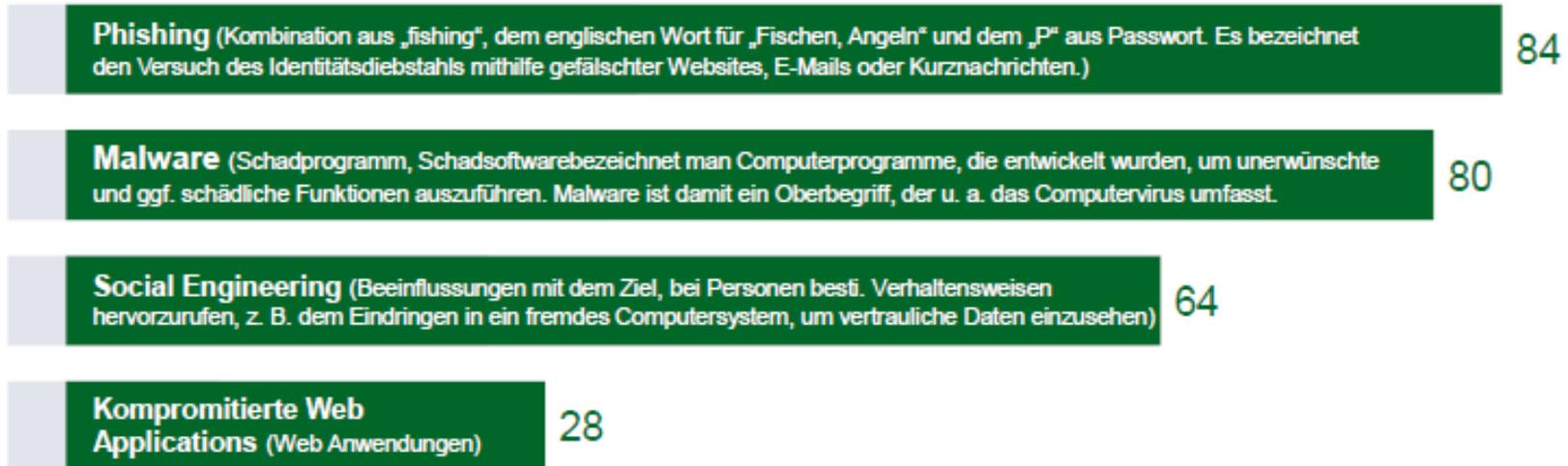
Jeder Freiberufler ist durch das Bundesdatenschutzgesetz (§ 9 BDSG) verpflichtet, alle erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, um Patienten-, Mandanten- oder Kundendaten zu schützen.

Besteht der Verdacht, dass diese Sorgfaltspflicht nicht gewahrt wurde, sehen sich Ärzte und Angehörige der rechtsberatenden Berufe mit einem Strafverfahren nach § 203 „Verletzung von Privatgeheimnissen“ konfrontiert.

## Mich betrifft das nicht...!?

Mehr als 70 % aller deutschen Unternehmen waren in den vergangenen zwei Jahren von Cyberkriminalität betroffen.

### Art von Cyber-Attacke auf Unternehmen in Prozent



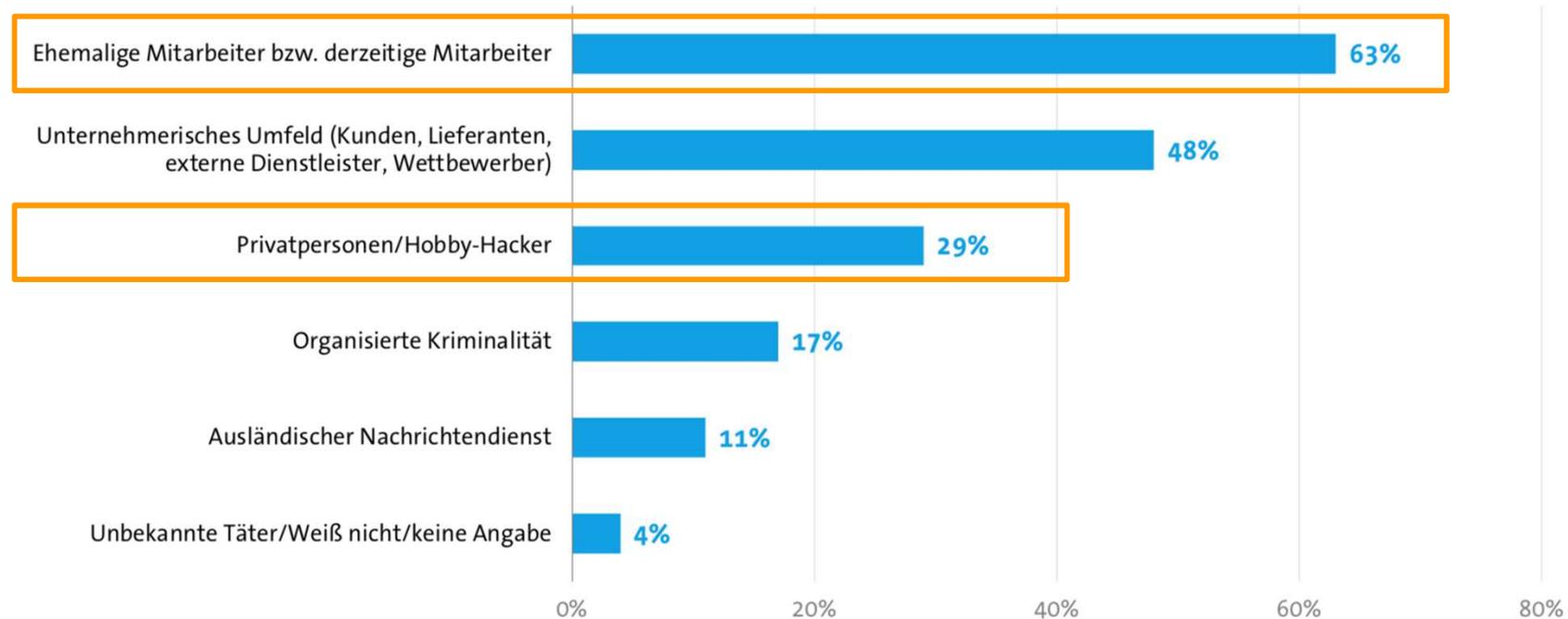
KPMG, Deutschland, 2016

46 % der Cybervorfälle werden durch die eigenen, zumeist ungeschulten Mitarbeiter verursacht!

# Mich betrifft das nicht...!?

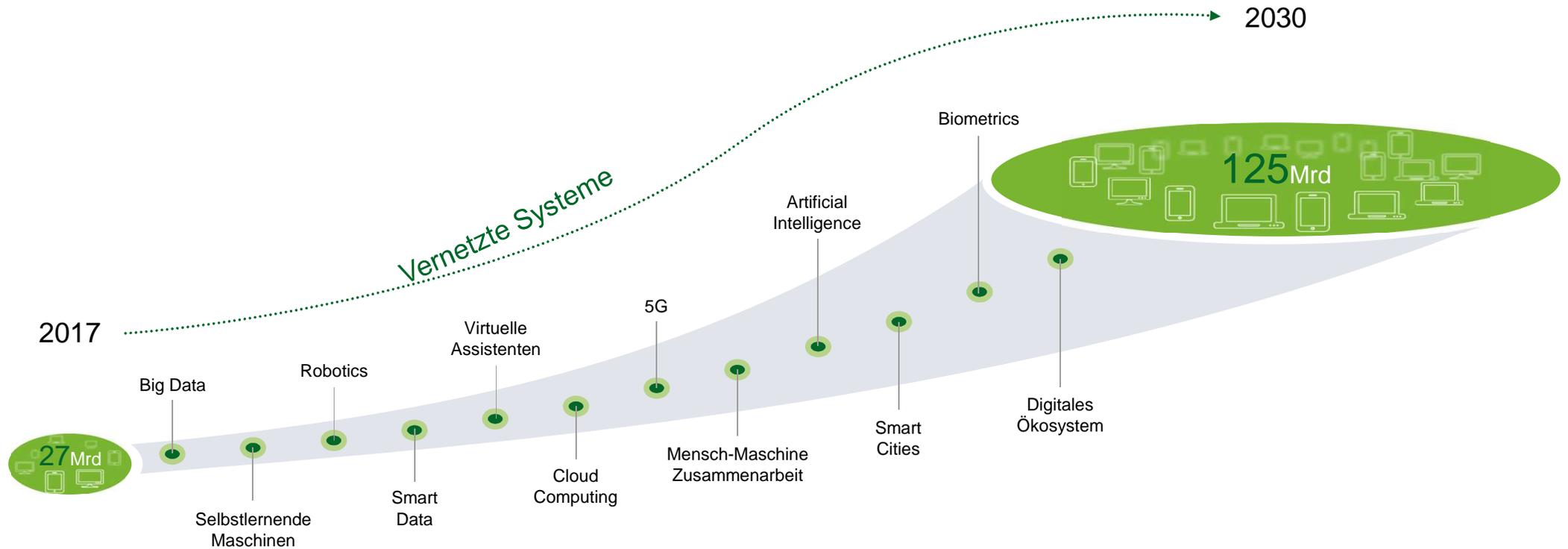
## 3 von 10 Angriffen stammen von Hobby-Hackern

Von welchem Täterkreis gingen diese Handlungen (vermutlich) in den letzten zwei Jahren aus?



Mehrfachnennung in Prozent

# Die Digitale Revolution erschafft eine hypervernetzte Welt



Mich betrifft das nicht...!?



Es passiert ca. alle 3 Minuten in Deutschland:  
Einbruch, Diebstahl, Vandalismus.

Dabei wird aufgebrochen, randaliert,  
gestohlen, zerstört, usw.

Schadensumme: **470 Millionen €**



Alle 16 Sekunden gibt es eine **erfolgreiche Attacke**  
auf IT Systeme in Deutschland.

**Auch hier** - Einbruch, Diebstahl, Vandalismus.

Dabei wird aufgebrochen, randaliert,  
gestohlen, zerstört, usw.

Schadensumme: **50 Milliarden €**

## Mich betrifft das nicht...!?

**Von:** Lasse Weber [mailto:weber.lasse.97@net-24.at]

**Gesendet:** Donnerstag, 24. März 2016 06:38

**An:** [REDACTED]

**Betreff:** Bewerbung

### **Bewerbung**

Sehr geehrter Herr [REDACTED],

da ich auf der Suche nach einer neuen beruflichen Herausforderung bin, möchte ich mich hiermit bei Ihnen um eine Stelle als Zerspanungsmechaniker bewerben, da ich bereits mehrere Jahre in diesem Bereich gearbeitet habe und zurzeit Arbeit suchend bin, möchte ich mich bei Ihnen bewerben.

Nach meiner Fachhochschulreife und meinen bisherigen Praktika konnte ich bereits Erfahrungen in unterschiedlichen Bereichen sammeln.

Sie finden in mir einen belastbaren, einsatzbereiten, flexiblen, selbstständigen und zuverlässigen Mitarbeiter mit hoher Teamorientierung. Das Einarbeiten in neue Aufgabengebiete bereitet mir keine Probleme.

Ich würde mich sehr freuen, wenn meine Bewerbung Ihr Interesse wecken konnte und ich mich persönlich bei Ihnen vorstellen darf. Über ein persönliches Gespräch freue ich mich sehr.

Mit freundlichen Grüßen

Lasse Weber

Anhänge

Zertifikate, Arbeitszeugnis u Lebenslauf

Die vollständige Bewerbungsmappe habe ich meine Dropbox geladen, weil die Datei für die Email zu groß war - Entschuldigen Sie bitte!

<https://www.dropbox.com/sh/bwcm143y5wmuwbd/AAC7DGJyas> [REDACTED]

Mich betrifft das nicht...!?



## Ihre persönlichen Dateien sind von CTB-Locker verschlüsselt.

Ihre Dokumente, Fotos, Datenbanken und andere wichtige Dateien mit stärkster Verschlüsselung und eindeutigen Schlüssel, die für diesen Computer generiert verschlüsselt wurden.

Privatentschlüsselungsschlüssel ist auf einem geheimen Internet-Server gespeichert und niemand kann Ihre Dateien entschlüsseln, bis Sie zahlen und den privaten Schlüssel erhalten.

**Sie haben nur 96 Stunden, die Zahlung zu einreichen. Wenn Sie Geld im vorgesehenen Zeitraum nicht senden, werden alle Ihre Dateien permanent verschlüsselt bleiben und niemand wird in der Lage sein, sie wiederherzustellen.**

Drücken Sie 'Ansicht', um die Liste der Dateien, die verschlüsselt wurden, anzusehen.

Drücken Sie auf 'Weiter' für die nächste Seite.

 **WARNUNG! VERSUCHEN SIE NICHT, DAS PROGRAMM SELBST LOSZUWERDEN. ALLE MAßNAHMEN WÜRDEN DEN ENTSCHLÜSSELUNGSSCHLÜSSEL FÜHREN ZERSTÖREN. SIE WÜRDEN IHRE DATEIEN FÜR IMMER VERLIEREN. NUR SO ZU HALTEN IHRE DATEIEN IST DIE ANWEISUNG ZU FOLGEN.**

**Ansicht**     **95 57 19**     **Weiter >>**

UP3ZAVK-L2UTNDY-5SCAKKM-OQHURGI-LUK6LRW-3YNDCCG-CBN4OCNP-D6GKGVA-W3B3DAH-BNDCK64-DT6R2HN-B5QVXBC-NBHLOD2-QITURPH-2642K4K-5A6X45I

Folgen Sie den Anweisungen auf dem Server.

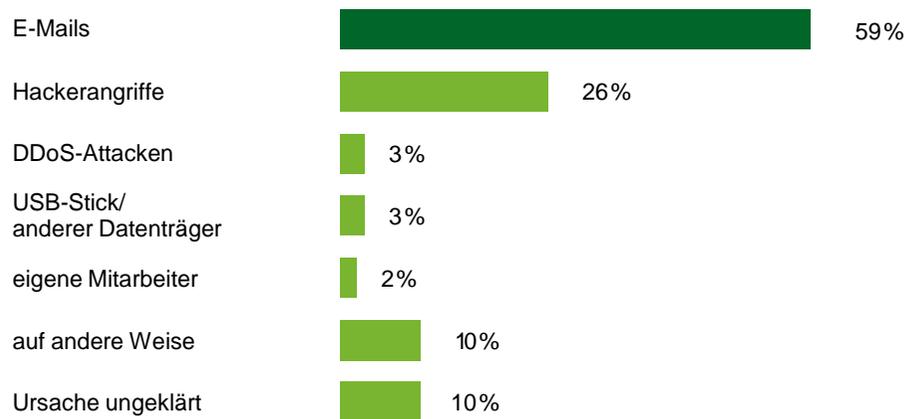
Diese Anleitung ist auch im Dokumentenmappe zu Datei benannt Decrypt-All-Files.txt gespeichert. Sie können es öffnen und verwenden Copy-Paste für Adresse und Schlüssel.

# Größtes Einfallstor für Cyberattacken sind E-Mails

Das E-Mail-Postfach ist für viele Unternehmen die wichtigste digitale Schnittstelle zu Kunden und Lieferanten. Cyberkriminelle nutzen aus, dass die elektronische Post samt Anhängen zu oft gedankenlos geöffnet wird – und legen mit ihrer Schadsoftware nicht nur die IT-Systeme, sondern ganze Betriebe lahm.

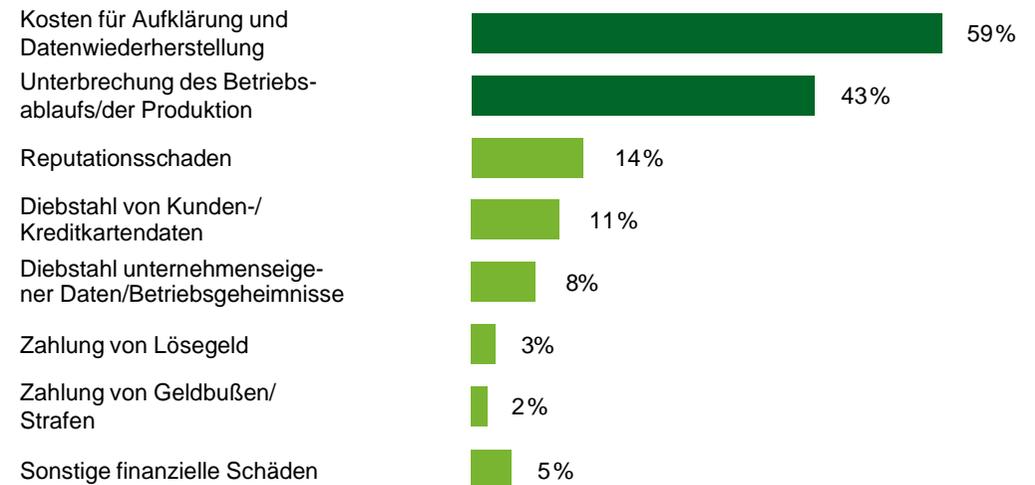
## Die Einfallstore

Erfolgreiche Cyberangriffe erfolgten durch ...<sup>1</sup>



## Die Schäden

Die Attacken führten zu wirtschaftlichen Schäden durch ...<sup>1</sup>



<sup>1</sup> Mehrfachnennungen möglich | Quelle: GDV, Forsa-Befragung Frühjahr 2018

# Wirkungsgrad von Anti-Viren-Scannern

Rank	1	2	3	4	5	6	7	8	9	10
	Bitdefender Antivirus plus 2018	BullGuard Antivirus 2018	Norton Security Deluxe	McAfee Antivirus 2018	Panda Antivirus 2018	Kaspersky Antivirus 2018	AVG Antivirus 2018	Avast! Pro Antivirus 2018	F-Secure Antivirus 2018	Norman Antivirus 2018
										
<b>Der niedrigste Preis:</b>										
	<a href="#">INFO</a>	<a href="#">INFO</a>	<a href="#">INFO</a>	<a href="#">INFO</a>	<a href="#">INFO</a>	<a href="#">INFO</a>	<a href="#">INFO</a>	<a href="#">INFO</a>	<a href="#">INFO</a>	<a href="#">INFO</a>
	29,99 €	29,95 €	49,99 €	29,95 €	32,99 €	31,95 €	39,99 €	39,99 €	39,95 €	40,95 €
Temporärer Rabattcode	25% Rabatt!	23,96 €	34,99 €		27,99 €					
<b>Anzahl der Computer:</b>										
Lizenz	3	1	1	1	1	1	1	1	1+	1+
<b>Sicherheits-Punktzahl:</b>										
Schutz-Punktzahl	99%	99%	98%	98%	97%	98%	93%	96%	95%	95%
<b>Verschiedene Funktionen:</b>										



# Ein erfolgreiches Anti-Viren-Programm...?

## Avast Antivirus verkauft massenhaft Browser-Daten seiner Nutzer

Über ein Tochterunternehmen soll der Antiviren-Software-Anbieter Avast massenhaft Browser-Daten von Nutzern verkauft haben.

Lesezeit: 1 Min.  In Pocket speichern

   502



(Bild: Avast)

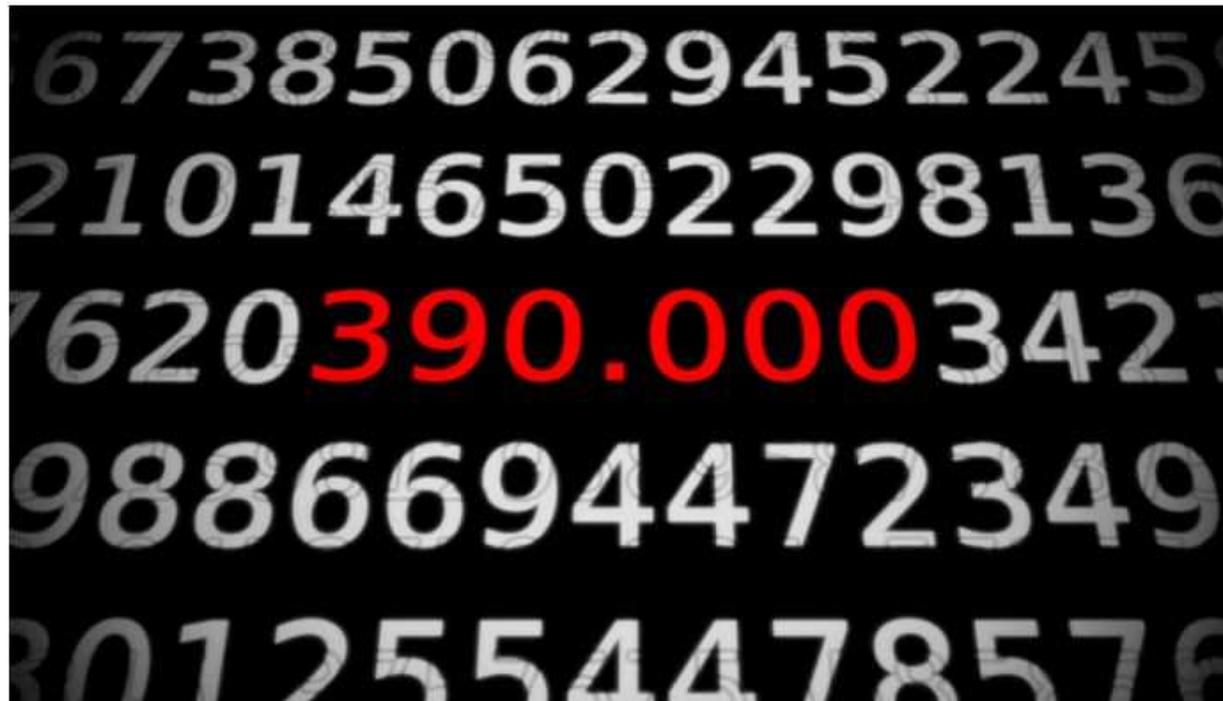
28.01.2020 11:23 Uhr

## Wirkungsgrad von Anti-Viren-Scannern

### Zahlen, bitte! Täglich 390.000 neue Schadprogramme

19.04.2016 13:43 Uhr - Jürgen Schmidt, Volker Zota

vorlesen



Momentan hat man das Gefühl, in jedem Mail-Anhang und hinter jedem Link versteckt sich irgendeine Malware. Antiviren-Hersteller und Test-Labore verstärken diesen Eindruck noch durch irrwitzig hohe Zahlen neuer Schadprogramme.

## Wirkungsgrad von Anti-Viren-Scannern

- Maximaler Wirkungsgrad 99%
  - 36-72 Stunden Zeitversatz durch updates
  - 390.000 neue Attacken im Netz täglich
- 3900 unbekannte Attacken pro Tag

**Ständiges Risiko von ca.  
12.000 unbekanntem Attacken**

## Brauchen Sie IT Kenntnisse?

The screenshot shows the 'Rent-A-Hacker' website with a dark theme. At the top, there are navigation links for 'Products', 'FAQs', 'Register', and 'Login'. Below the navigation is a search bar containing 'Rent-A-Hacker'. The main content is a table listing various hacking services, their prices in EUR and Bitcoin (฿), and a 'Buy now' button for each. The services include small jobs (250 EUR), medium-large jobs (500 EUR), large jobs (900 EUR), and an upgrade for instant replies (200 EUR).

Product	Price	Quantity
Small job, for example: Email and Facebook hacking, installing trojans, small DDOS	250 EUR = 0.03820 ฿	1 X Buy now
Medium-large job, ruining people, espionage, website hacking, DDOS for big websites	500 EUR = 0.07640 ฿	1 X Buy now
Large job which takes a few days or multiple smaller jobs, DDOS for protected sites	900 EUR = 0.13752 ฿	1 X Buy now
UPGRADE: INSTANT reply within 30-60 minutes instead of 24-36 hours for urgent cases. If i need longer this will get refunded. Only buy this together with one of the other options.	200 EUR = 0.03056 ฿	1 X Buy now

had people make things you wouldn't believe really often.  
- A lot of experience with security practices inside big corporations.

Mich betrifft das nicht...!?

Cyber-Versicherung: Risikoeinschätzung EU Datenschutzgrundverordnung

26.03.2018

EU-Datenschutzrecht

## Warum künftig hohe Strafen bei Datenlecks drohen

Einen Hack lieber unter den Teppich kehren? Das war noch nie eine gute Idee. Ab Mai könnte das richtig teuer werden. Auch kleine und mittlere Unternehmen müssen bei Verlust von Kundendaten schnell handeln, wenn sie keine hohen Strafen riskieren wollen.

EU-Bürgern

72 Stunden melden.



## Aktuelles

› DATEV news

› Nachrichten Steuern & Recht

› DATEV-Blogs

› **Trends und Innovationen**

› Kundenzeitschriften

› Veranstaltungen

› Newsletter

› Rund um die DATEV-Programme

› RSS

› Kommunikationsmaßnahmen an Ihre Mandanten

Versicherungen gegen IT-Risiken

## Cyber Versicherungen als Ergänzung der IT-Sicherheit

Der Markt für Cyber Insurances, also Versicherungen gegen Cyber-Risiken, blüht. Kein Wunder, denn das Risiko Opfer eines Hackerangriffs, einer Ransomware-Attacke oder einer DDoS-Erpressung (Distributed denial of service) zu werden, steigt kontinuierlich und IT-Sicherheitsvorfälle sind kostspielig.

Die durchschnittlichen Kosten einer Datenpanne betragen in Deutschland im Jahr 2017 3,42 Millionen Euro, so die „Cost of Data Breach“-Studie 2017 des Ponemon Instituts. Dies bedeutet zwar einen Rückgang der Kosten um 5,4 Prozent im Vergleich zum Vorjahr. Kommt es zu einem Security Breach (IT-Sicherheitsvorfall), können die wirtschaftlichen Folgen aber weiterhin schwerwiegend sein: Neben den Kosten für die Wiederherstellung von Daten und IT-Systemen sind es mögliche Vertragsstrafen, Haftungsfälle, Imageschäden, Kunden- und Umsatzverlust, die zu den finanziell spürbaren Konsequenzen gehören.

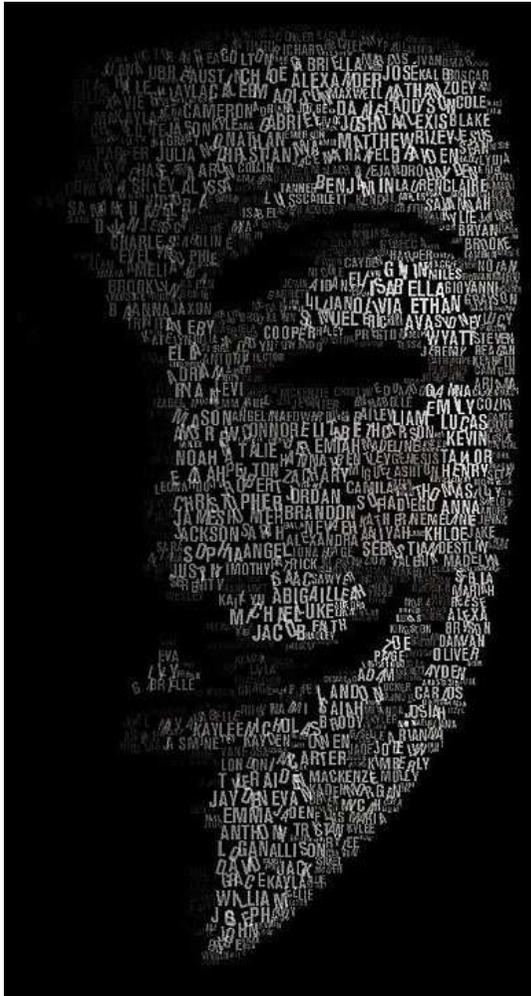
Werden gesetzliche Vorgaben verletzt, können Bußgelder und Strafverfahren hinzukommen. Sind personenbezogene Daten betroffen (Data Breach), kann es in naher Zukunft sehr teuer werden.

## Versicherungen gegen Restrisiken

Leider liegt die Wahrscheinlichkeit, dass es zu einem IT-Sicherheitsvorfall oder zu einer Datenpanne kommt, bei weitem über null Prozent. Viele Security-Experten können es kaum noch hören, aber es stimmt: Es gibt keine hundertprozentige Sicherheit. Um den verbleibenden Risiken, den Restrisiken, zu begegnen, schließt man Versicherungen ab, das gilt nicht nur für Firmengebäude und Fuhrpark, sondern auch für die IT und den Cyber-Raum.

Cyber-Versicherungen oder IT-Versicherungen sollten als möglicher Baustein eines Cyber-Security-Konzeptes verstanden werden: Auf Basis der Risikoanalyse werden Schutzbedarf und zugehörige Schutzmaßnahmen definiert. Wenn sich kein ausreichender Schutz durch die Cyber-Security finden

## Restrisiken...



**Das Restrisiko ist das  
Risiko, dass Ihrer Kanzlei  
den Rest gibt!**

Schutzmaßnahmen definiert. Wenn sich kein ausreichender Schutz durch die Cyber-Security finden lässt, kommen Cyber Insurances zur Absicherung der Restrisiken in Betracht.

ENISA, die EU-Agentur für Netz- und Informationssicherheit, hat bereits vor vielen Jahren in einer Studie (<https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe>) darauf hingewiesen, dass Cyber-Versicherungen einen Vorteil für die Entwicklung der Cyber-Sicherheit bringen können.

## Cyber-Risiken sind Top-Risiken für Unternehmen

Die Versicherungsgesellschaften haben die Cyber-Risiken ebenfalls schon länger im Blick. Studien wie das Allianz Risk Barometer zeigen seit Jahren, dass Cyber-Vorfälle zu den größten Unternehmensrisiken in Deutschland gezählt werden. Der Versicherungsmarkt hält entsprechend eine Reihe von Angeboten für Unternehmen vor.

## Darknet Insurance: Selbst die Angreifer versichern sich

Wie weit das Thema der Cyber-Versicherungen bereits fortgeschritten ist, zeigte ein Vortrag von Ladi Adefala, Senior Security Strategist bei Fortinet, bei der Information Security World 2017: So gibt es bereits Versicherungsangebote im Darknet, mit denen sich Cyber-Kriminelle absichern können. Wenn zum Beispiel eine Attacke mit einem empfohlenen Angriffswerkzeug nicht funktioniert, dann springt die Darknet Insurance für den Schaden ein.

Erst recht sollten Unternehmen daran interessiert sein, ihre Cyber Security mit passenden Cyber Insurances zu ergänzen. Teilweise gibt es die Security-Lösungen bereits im Paket mit einer Versicherung.

Autor: Oliver Schonschek

(c)2017 Vogel Business Media



### Bitte beachten Sie

Die Beiträge in der Rubrik "Trends und Innovationen" sind Inhalte unseres Medienpartners Vogel Business Media. Sie spiegeln nicht unbedingt die Meinung von DATEV wider.

> Vogel Business Media



## Aktuelles

- > [DATEV news](#)
- > [Nachrichten Steuern & Recht](#)
- > [DATEV-Blogs](#)
- ▼ [Trends und Innovationen](#)
- > [Kundenzeitschriften](#)
- > [Veranstaltungen](#)
- > [Newsletter](#)
- > [Rund um die DATEV-Programme](#)
- > [RSS](#)
- > [Kommunikationsmaßnahmen an Ihre Mandanten](#)

Ransomware unter der Lupe

## 3.700 Euro Lösegeld für die Daten

Die durchschnittliche Lösegeldforderung bei einem Ransomware-Angriff liegt laut einer aktuellen Umfrage bei 3.700 Euro. Die durchschnittlich mit einem Angriff verbundenen Kosten sind jedoch um mehr als den Faktor zehn höher.

Der Ransomware Report, für den weltweit 2.400 Managed Service Provider über deren knapp eine halbe Million Kunden aus dem KMU-Segment (kleine und mittlere Unternehmen) befragt wurden, skizziert die Auswirkungen auf kleine und mittelgroße Unternehmen durch Ransomware-Angriffe. Der Initiator der Studie, Hersteller Datto, legt nahe, dass einhergehender Umsatzverlust durch Ausfallzeiten geschäftsbedrohende Ausmaße annehmen kann. Eine durchschnittliche Attacke kostet ein Unternehmen demnach mehr als zehnmal so viel wie das geforderte Lösegeld. So kostet laut der Erhebung ein Angriff im Durchschnitt 40.500 Euro. Das durchschnittlich geforderte Lösegeld liegt bei 3.700 Euro pro Angriff – unabhängig davon, ob es gezahlt wurde oder nicht.

### Attacken halten an

Mit 55 Prozent teilten etwas mehr als die Hälfte der befragten MSPs mit, dass ihre Kunden im ersten Halbjahr 2018 eine Ransom-Attacke hinnehmen mussten. 35 Prozent der Umfrageteilnehmer aus dem Kreis der Managed Service Provider (MSP) sagen, dass ihre Kunden sogar mehrfach an einem Tag angegriffen werden. Für 92 Prozent der Dienstleister ist absehbar, dass die Anzahl der Attacken gleich hoch bleibt oder sogar steigen wird.

85 Prozent der Ransomware-Opfer hatten eine Antiviren-Lösung im Einsatz. 65 Prozent hatten einen Spam-Filter in Betrieb. 29 Prozent gaben an, dass die Opfer Pop-up-Blocker im Einsatz hatten.

### Dunkelziffer ist hoch

## Aktuelles

- > DATEV news
- > Nachrichten Steuern & Recht
- > DATEV-Blogs
- ▼ Trends und Innovationen
- > Kundenzeitschriften
- > Veranstaltungen
- > Newsletter
- > Rund um die DATEV-Programme
- > RSS

Worldwide Infrastructure Security Report

## Hackerangriffe kosten richtig Geld

Unternehmen sind sich der steigenden Gefahren durch Cyberkriminelle bewusst und verschlüsseln ihren Datenverkehr zunehmend. Dies spiegelt sich auch in den Angriffsmustern von Hackern wieder. 94 Prozent der von Netscout weltweit befragten Unternehmen geben an, dass sie im vergangenen Jahr Angriffe auf ihren verschlüsselten Traffic verzeichnet haben. Dies sind fast doppelt so viele im Vergleich zum Vorjahr.

2018 wurde der bisher größte DDoS-Angriff mit 1,7 Terabit pro Sekunde gemessen. Und es zeigt sich, Angriffstechniken entwickeln sich kontinuierlich weiter. So war bei 91 Prozent der Unternehmen, die 2018 eine derartige Attacke verzeichnet haben, mindestens eine ihre Internet-Bandbreite vollständig überlastet. Das kam beim „WorldwideInfrastructureSecurity Report“ (WISR) von Netscout heraus.

Die Angreifer setzten dem Bericht zufolge vor allem auf DDoS-Offensiven, die die Infrastrukturen sowie Firewalls und IPS-Geräte von Unternehmen beeinträchtigen. Diese Angriffe sind von 16 Prozent (2017) auf 31 Prozent (2018) gestiegen. Ziel der Hacker ist es dabei, Internet-Services, IT-Komponenten oder die IT-Infrastruktur eines attackierten Unternehmens zu verlangsamen, gänzlich lahmzulegen oder zu beschädigen.

## Enorme Kosten für Ausfallzeiten

Die durchschnittlichen Kosten, die ein Unternehmen pro Stunde Ausfallzeit aufgrund von DDoS-Angriffen 2018 zu erwarten hatte, betragen weltweit knapp 201.000 Euro. Deutsche Unternehmen liegen deutlich über diesem Schnitt und verzeichneten 323.400 Euro pro Stunde Ausfallzeit.

# [www.sicherheitstacho.eu](http://www.sicherheitstacho.eu)



# Schadenfälle

## Schadenfall E-Mail

- Autovervollständigen in Outlook wurde nicht geprüft
- 200 Kundendaten wurden an einen außenstehenden Dritten gemailt
- Der Vorfall war mehrere Tage in diversen Medien

Folgende Kosten sind entstanden:

▪ IT Forensik	13.000,-€
▪ Kosten für die rechtliche Betreuung der Betroffenen	60.000,-€
▪ Kosten für die Informationen an die Betroffenen & Call Center	15.000,-€
▪ <b>GESAMTSCHADEN:</b>	<b>88.000,-€</b>

# Schadenfälle

## Schadenfall Ransomware im Hotel

Mitarbeiter öffnen eine Mail eines vermeintlichen Kunden und klicken auf den Anhang der Mail

- Dadurch wurde ein Verschlüsselungstrojaner aktiviert
- Sämtliche Daten wurden verschlüsselt
- Durch die Verschlüsselung waren die Code-Karten unbrauchbar und die Zimmertüren ließen sich nicht mehr öffnen

Folgende Kosten sind entstanden:

- |   |           |
|---|-----------|
| ▪ Lösegeld                                  | 35.000,-€ |
| ▪ Bewirtung der Gäste während der Wartezeit | ??        |

Was hätte die Cyber Versicherung bezahlt:

- Wiederherstellung des Regelbetriebes
- IT Beratung & Forensik
- Betriebsunterbrechungsschaden
- Lösegeld

**Durch das Awarenessstraining & den Werkzeugkasten von PERSEUS  
wäre dieser Schaden vermutlich gar nicht entstanden.**

# Schadenfälle

The image displays two screenshots of ransomware interfaces. The left screenshot is for Wana Decrypt0r 2.0, which has a dark red background. It features a padlock icon and a message in German: "Oops, your files have been encrypted!". It includes a countdown timer for payment (02:23:53:12) and a warning that files will be lost if payment is not made by 07/27/2017 03:01:12. The interface provides instructions on how to recover files by paying \$300 in Bitcoin to a specific address: 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw. The right screenshot is for CryptoLocker-v3, which has a red background. It features a shield icon and a message: "Your personal files are encrypted!". It includes a countdown timer for private key destruction (7/23/2017) and a warning that the private key will be destroyed. The interface provides instructions on how to recover files by paying a Bitcoin address: 1LSHFdm1EPVf7v8723MchxvwLAJe41TMYT. Both interfaces include buttons for "Check Payment" and "Decrypt" or "Enter Decrypt Key".

**Wana Decrypt0r 2.0**

Oops, your files have been encrypted!

Was geschah mit meinem Computer?  
Ihre wichtigen Dateien sind verschlüsselt. Viele Ihrer Dokumente, Fotos, Videos, Datenbanken und andere Dateien sind nicht mehr zugänglich, weil sie verschlüsselt wurden. Vielleicht sind Sie damit beschäftigt, einen Weg zu finden, um Ihre Dateien wiederherzustellen, aber verschwinden Sie nicht Ihre Zeit. Niemand kann Ihre Dateien ohne unseren Entschlüsselungsdienst wiederherstellen.

Kann ich meine Dateien wiederherstellen?  
Sicher. Wir garantieren, dass Sie alle Ihre Dateien sicher und einfach wiederherstellen können. Aber du hast nicht genug Zeit. Sie können einige Ihrer Dateien kostenlos entschlüsseln. Versuchen Sie jetzt, indem Sie auf <Decrypt> klicken. Aber wenn du alle deine Dateien entschlüsseln willst, musst du bezahlen. Sie haben nur 3 Tage, um die Zahlung einzureichen. Danach wird der Preis verdoppelt. Auch wenn du nicht in 7 Tagen bezahlt hast, kannst du deine Dateien nicht für immer wiederherstellen. Wir haben freie Veranstaltungen für Benutzer, die so arm sind, dass sie nicht in 6 Monaten bezahlen können.

Wie bezahle ich?  
Die Zahlung wird nur in Bitcoin akzeptiert. Für weitere Informationen klicken Sie auf <About bitcoin>.

Send \$300 worth of bitcoin to this address:  
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Payment will be raised on 7/23/2017 03:01:12  
Time Left 02:23:53:12

Your files will be lost on 7/27/2017 03:01:12  
Time Left 06:23:53:12

Check Payment Decrypt

**CryptoLocker-v3**

Your personal files are encrypted!

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key**.

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.

Once this has been done, nobody will ever be able to restore files...

In order to decrypt the files open your personal page on site <https://34r6hq26q2h4jkzj.tor2web.fi> and follow the instruction.

Use your Bitcoin address to enter the site:  
1LSHFdm1EPVf7v8723MchxvwLAJe41TMYT

Click to copy Bitcoin address to clipboard

if <https://34r6hq26q2h4jkzj.tor2web.org> is not opening, please follow the steps: You must install this browser [www.torproject.org/projects/torbrowser.html.en](http://www.torproject.org/projects/torbrowser.html.en) After installation, run the browser and enter address [34r6hq26q2h4jkzj.onion](https://34r6hq26q2h4jkzj.onion) Follow the instruction on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

Show encrypted files Check Payment Enter Decrypt Key

Click to Free Decryption on site

# Kosten einer Cyber Attacke

- durchschnittlich 46 000 Euro bei Kleinunternehmen
- durchschnittlich 342 000 Euro bei Großunternehmen
- **IT-Forensik** 300 Euro/Stunde  
Der Einsatz dieser Spezialisten kann mehrere Tage dauern -> bei 50 Stunden ergeben sich 15 000 Euro
- **Wiederherstellung der IT-Systeme**  
Unterstützung durch externe IT-Dienstleister des Händlers -> rund 10 000 Euro
- **Rechtsanwaltliche Beratung bei einem Datenschutzvorfall**  
400 Euro/Stunde -> bei 50 Stunden ergeben sich 20 000 Euro
- **Benachrichtigung betroffener Kunden**  
2,50 Euro pro Datensatz -> bei 20 000 Kundendatensätzen ergeben sich 50 000 Euro
- **Verletzung von PCI-Vertragspflichten (Kreditkartensicherheit)**  
25 000 Euro bis 300.000 Euro
- **Schadensersatzkosten**  
Haftpflichtanspruch von Kunden, deren Persönlichkeitsrechte verletzt wurden.
- **Ertragsausfall**  
Bestellungen, die über den Online-Shop fünf Tage lang nicht angenommen werden können; Kassen, die im stationären Handel nicht funktionieren: 1–2 Prozent des Jahresumsatzes

Quelle: Hiscox Report 2018;

# Agenda

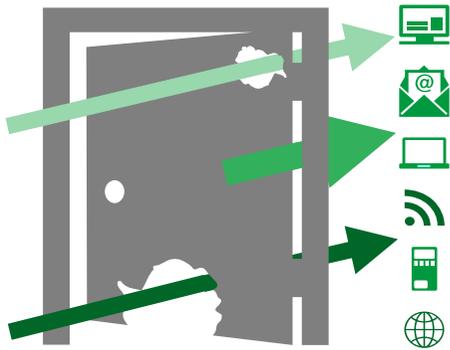
- 1 HDI stellt sich vor
  - Ihre Ansprechpartner
- 2 Ausgangs- und Bedrohungslage
- 3 Das Cyber-Security-Konzept
- 4 Kosten / Prämien
- 5 Fragen
- 6 Fazit

## Der richtige Schutz???



# der richtige Schutz!!!

## Das umfassende Cyber-Security-Konzept von HDI und Perseus



### technische Maßnahmen im Unternehmen

- Virenschutz
- Firewall
- Datensicherung

aber selbst die beste  
Technik ist wertlos, wenn  
Mitarbeiter  
unverantwortlich handeln.



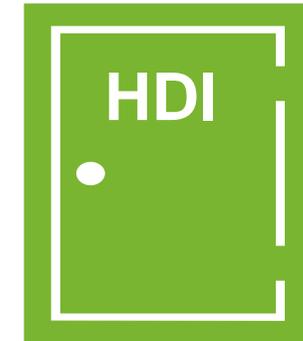
### organisatorische & personelle Maßnahmen

- Cyberführerschein und Datenschutz-Führerschein für alle Mitarbeiter
- fingierte Hackerangriffe
- Werkzeugkasten für Cybersicherheit
- IT-Sicherheitsreport und Trainingsreporting



### HDI Cyberversicherung

- 7/365 Hotline
- Notfallberatung und erste Schadenerfassung
- Vor-Ort-Support innerhalb von 24 Stunden
- Wiederherstellung von Daten
- Forensik & Beweissicherung



### HDI Cyberversicherung

- Assistanzenleistungen
- Kosten
- Drittschäden
- Eigenschäden

# Das umfassende Cyber-Security-Konzept von Perseus



**Eine 360°-Lösung für  
Cyber Security.**

**perseus.**



**Nachhaltiges Training &  
Dauerhafter Schutz**

**Cyberführerschein**

**Datenschutz-Führerschein**

**fingierte Hackerangriffe**

**Werkzeugkasten für Cybersicherheit**

# Cyber-Security- as a Service



**Cybersicherheit ist keine einmalige Aktion – es ist ein laufender Prozess.**

Eine Plattform mit allen Bausteinen zur Cybersicherheit und Datenschutz.



**... für alle**

- Trainingsbereich
- Werkzeugkasten für Cybersicherheit
- aktive Informationen
- Angriffsalarm



**... für den Inhaber/IT-Verantwortlichen**

- Mitarbeiterübersicht
- Reporting-Bereich für Trainingsstatistik und Cyber-Sicherheit
- Scoring-Bericht – Status-Quo incl. Handlungsempfehlungen zur Steigerung der Cybersicherheit



# Das umfassende Cyber-Security-Konzept von Perseus

**Unsere Mission ist es, jeden Mitarbeiter zu befähigen, aktiv zur Cybersicherheit beizutragen.**

**Bei Perseus steht der Mensch im Mittelpunkt.**



- ✓ Nachhaltiges Training
- ✓ Dauerhafter Schutz

## Exkurs – andere Anbieter



# Produktinformationen auf einen Blick

## Die Cyber-Versicherung bietet Unternehmen Versicherungsschutz für

- **Eigenschäden: Kosten, Serviceleistungen und Betriebsunterbrechung**
- **Drittschäden**

<b>Versicherungssummen</b>	100.000 Euro, 250.000 Euro, 500.000 Euro, 750.000 Euro, 1.000.000 Euro einfache Jahresmaximierung
<b>Selbstbeteiligungen</b>	1.000 Euro (Standard) oder 2.500 Euro sowie zeitlichen SB von 12 Std. bei BU
<b>Geltungsbereich</b>	Weltweit <b>NEU</b>
<b>Laufzeit</b>	1 Jahr (mit automatischer Verlängerung)
<b>Priorität</b>	<b>Die Cyberversicherung (Stand-alone) geht immer vor</b>

# Produktinformationen auf einen Blick

## Eigenschäden

### Kosten und Serviceleistungen

- Soforthilfe im Krisenfall – **erste 90 Minuten ohne Selbstbehalt**
- Forensik und Schadenfeststellung
- Sofern kein Versicherungsfall:  
48 Std. ohne Anrechnung des Selbstbehalts

### Versicherte Kosten im Schadenfall

- Benachrichtigungskosten und Callcenter
- Krisenkommunikation und PR-Maßnahmen
- Kosten für Datenüberwachungsdienstleistungen
- Systemverbesserungen
- Abwehr einer Cybererpressung inkl. z.B. Belohnungsgelder, Vertrauensschäden



### Wiederherstellungskosten

- Entfernung von Schadsoftware
- Wiederherstellung gelöschter/geschädigter Daten, Software, Netzwerke und Webseiten

### Betriebsunterbrechung/Ertragsausfall

#### Ersatz von

- Entgangenem Betriebsgewinn
- Fortlaufenden Kosten bei Vorliegen einer Netzwerksicherheitsverletzung
- Betriebsunterbrechung durch Datenverlust als Folge eines Bedienfehlers

# Produktinformationen auf einen Blick

## Drittschäden

- Prüfung der Haftpflichtfrage
- Abwehr unberechtigter Schadenersatzansprüche
- Freistellung des Versicherungsnehmers von berechtigten Schadenersatzverpflichtungen
  
- Rückwärtsdeckung unbegrenzt
- Nachmeldefrist 5 Jahre



## Deckungserweiterungen

- Unberechtigte Veröffentlichung elektronischer Medienhalte
- Forderungen zur Zahlung von Vertragsstrafen durch E-Payment-Service-Provider
- Verteidigung in Datenschutzverfahren
- Erstattung von ausländischen Bußgeldern wegen Datenschutzverletzungen, soweit rechtlich zulässig
- Vertragsstrafen wegen Datenvertraulichkeitsverletzungen
- Immaterielle Schäden z.B. wegen Persönlichkeitsrechtsverletzungen sowie psychischen Beeinträchtigungen
- Vertragliche Freistellungsverpflichtungen gegenüber Auftragsdatenverarbeitern
- Erweiterte vertragliche Schadenersatzansprüche (vergebliche Aufwendungen im Vertrauen auf ordnungsgemäße Vertragserfüllung/ Mehraufwendungen wegen Verzögerung der Leistung )

# SYRISO

## Ein starker Dienstleister im Schadenfall

### Leistungsspektrum SYRISO

- Bereitstellung einer Hotline mit garantierten Reaktionszeiten zur Erstmeldung von Vorfällen
- Schadeneindämmung
- Krisenmanagement und Koordination von Maßnahmen der Rechtsberatung
- Begleitung der sicheren Wiederherstellung des Geschäftsbetriebs
- Aufklärung und Aufarbeiten von Cybervorfällen
- Maßnahmen zur Erkennung eines erneuten Aufflammens eines Vorfalls



**Cyberschaden-Hotline**  
0511 3031-562

Bedingungsgemäße Übernahme der anfallenden Kosten, ggf. unter Berücksichtigung einer vereinbarten Selbstbeteiligung

Bei Bedarf binnen 24 Std. beim Kunden vor Ort  
SEC Consult zertifiziert nach BSI-Standard

HDI: Akzeptanz und Kostenübernahme von firmeneigenen IT-Dienstleistern!

## Worauf Sie sich im Schadenfall verlassen können...



# Agenda

- 1 HDI stellt sich vor
  - Ihre Ansprechpartner
- 2 Ausgangs- und Bedrohungslage
- 3 Das Cyber-Security-Konzept
- 4 Kosten / Prämien
- 5 Fragen
- 6 Fazit

# Was kostet das Cyber-Security-Konzept?

## HDI Cyberversicherung

Umsatz in Euro	Deckungssumme in Euro				
	100.000	250.000	500.000	750.000	1.000.000
0 – 150.000	312	430	559	643	739
150.001 – 300.000	337	464	604	694	798
300.001 – 500.000	380	525	682	785	902
500.001 – 750.000	437	603	785	902	1.038
750.001 – 1.000.000	481	664	863	992	1.141
1.000.001 – 1.500.000	577	797	1.036	1.191	1.370
1.500.001 – 2.000.000	635	876	1.139	1.310	1.507
2.000.001 – 2.500.000	698	964	1.253	1.441	1.657
2.500.001 – 3.000.000	754	1.041	1.353	1.556	1.790
3.000.001 – 4.000.000	792	1.093	1.421	1.634	1.879
4.000.001 – 5.000.000	848	1.170	1.520	1.749	2.011

- Standardrisiko ohne optionale Deckungen; SB 1.000,-€

# Agenda

- 1 HDI stellt sich vor
  - Ihre Ansprechpartner
- 2 Ausgangs- und Bedrohungslage
- 3 Das Cyber-Security-Konzept
- 4 Kosten / Prämien
- > 5 Fragen
- 6 Fazit

## Impulsfragen

- **Wie sieht Ihr Krisenplan bei einer Datenpanne aus?**
- **Wen rufen Sie bei einem Hackerangriff an?**  
**Werden alle Sicherheitsmaßnahmen von DATEV lückenlos genutzt?**
- **(Zweifaktor Authentifizierung per App und per Smartcard; E-mail-Verschlüsselung, usw.)**
- **Welche Systeme/Programme nutzen Sie außerhalb von DATEV?**
- **Wie erfolgt die Mandantenkommunikation?**
- **Wie erfolgt die Arbeitszeiterfassung? – EuGH Urteil 14.05.2019**

## weitere Fragen



# Agenda

- 1 HDI stellt sich vor
  - Ihre Ansprechpartner
- 2 Ausgangs- und Bedrohungslage
- 3 Das Cyber-Security-Konzept
- 4 Kosten / Prämien
- 5 Fragen
- > 6 Fazit

## Fazit – Warum HDI?

- Deckungsbaustein „Spionage“
- Update-Garantie der Bedingungen
- Private Endgeräte mitversichert – auch mobile
- Keine „Stand der Technik“ Klausel
- Einbindung eigener IT Dienstleister
- kein SB in den ersten 90 Minuten
- Datensicherung einmal wöchentlich
- Können Sie selbst versichert werden?

→ **Sie kaufen keine Versicherung, sondern eine Problemlösung!**

**VersicherungsJournal.de**

Nachricht aus Versicherungen & Finanzen vom 22.10.2018

### Die besten Cyber-Versicherungen

Franke und Bornberg hat ein erstes Rating von Policen gegen Computerkriminalität vorgelegt. Darin liegen AIG, HDI, Hiscox und Markel an der Spitze. Allerdings konnte kein Anbieter die Höchstnote erzielen. Im Vergleich waren 34 Cyber-Tarife für kleine und mittelständige Unternehmen (KMU) von 28 Gesellschaften.

**HDI**



**HDI – als erster deutscher Anbieter mit Top Platzierung**