Markel Pro Cyber

Ein Webinar für Fortgeschrittene

Markel Insurance SE
Sophienstraße 26 | 80333 München | Telefon: +49 89 8908 316 50 | www.markel.de | service@markel.de

Cyberkriminalität ist die größte Bedrohung für jedes Unternehmen auf der Welt.

*Ginni Rometty, CEO von IBM

Ihr heutiger Referent

Marius Dressel

Position
Junior Underwriter

Ausbildung
Abgeschlossenes BWL-Studium an der Fachhochschule Rosenheim, Studium Digitale Innovation und Business Transformation an der Steinbeis-Hochschule

Bereiche
Financial Lines Versicherungsprodukte (u.a. D&O), Vermögensschadenhaftpflicht, Spezialkonzepte (Cyber und Vereine), Berufshaftpflichtversicherung (RSW)

Markel als Arbeitsplatz
Junger Versicherer mit hohem Potenzial

Zugehörigkeit
Seit März 2018 bei Markel

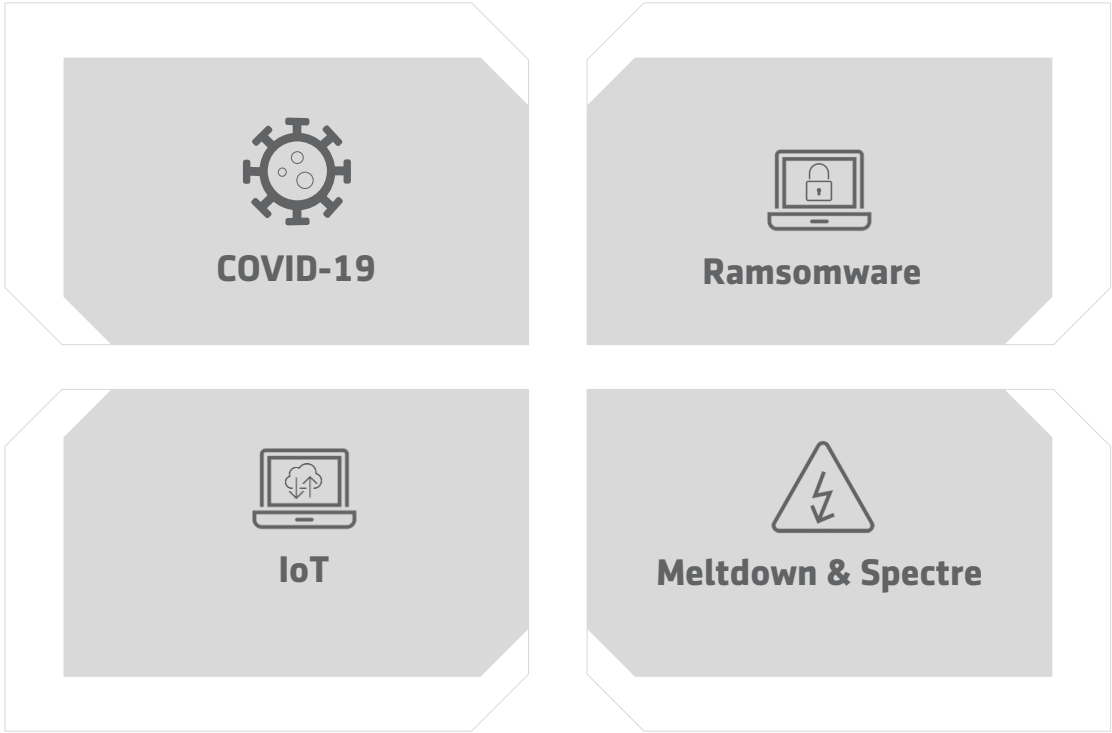
01 Ihre Kunden, ihre Risiken

Cyberrisiken

Neue Herausforderungen für Ihre Kunden

COVID-19

Erhöhte Anzahl an Hacker-Angriffe aufgrund der Tätigkeit im Home Office



Anstieg von Ransomware Attacken

Unternehmen sind heutzutage einer großen Anzahl von Cyberrisiken ausgesetzt (Hacking, Phishing, DDOS etc.)

Internet of Things (IoT)

Vernetzte Geräte (auch Wearables) führen zu großen Sicherheitslücken

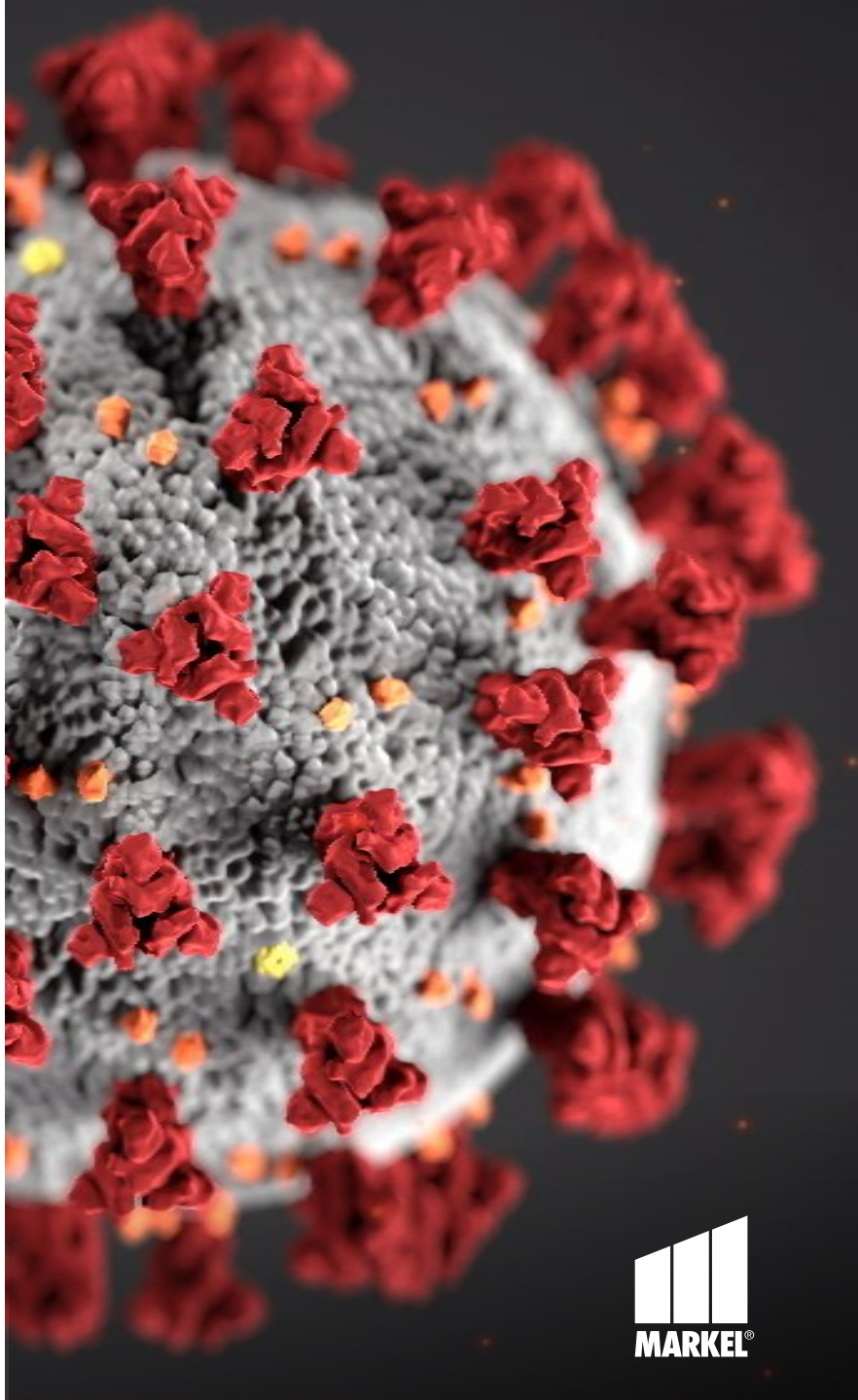
Meltdown und Spectre

Hardware-Hacks der Schwachstellen der Prozessoren der IT-Systeme

Erhöhte Gefahr von Cyberattacken in der Corona-Krise

Der digitale Virus greift die Cybersicherheit an

- Unzureichende IT-Kapazitäten
- Nicht ausreichend gesicherte VPNs (Virtual Private Networks)
- Fehlende Datenregulierungen
- Kein gesichertes Netzwerk
- Gebrauch von privaten IT-Systemen ohne Überprüfung von Datenschutz
- Mangelnde Datenschutzschulungen über das Arbeiten im Home Office

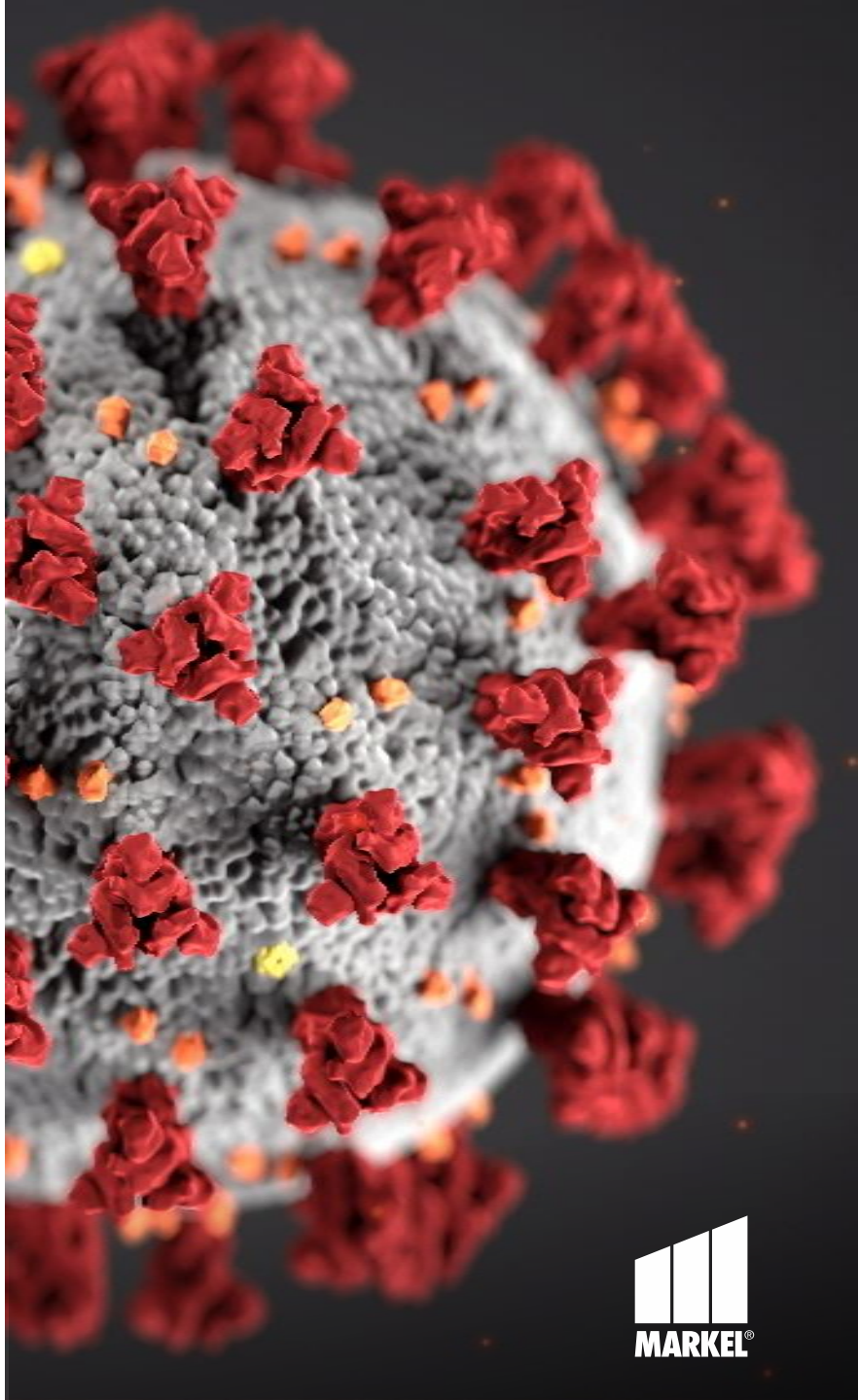


Die Cyberversicherung im Home Office

Markel Pro Cyber im Home Office

- ✓ Geltungsbereich der Cyberversicherung weltweit
- ✓ Vorbeugende Sensibilisierung der Mitarbeiter
- ✓ Mitversicherung der IT-Systeme und Daten des Arbeitgebers
- ✓ Mitversicherung des Zugriffs auf Programme und Daten des Arbeitgebers mit einem privaten Gerät

Tipp: Jedoch müssen die Mindeststandards an IT-Sicherheit auch im Home Office eingehalten werden. Das bedeutet auch für den Arbeitsplatz im Home Office müssen folgende Sicherheitssysteme aktiv sein.

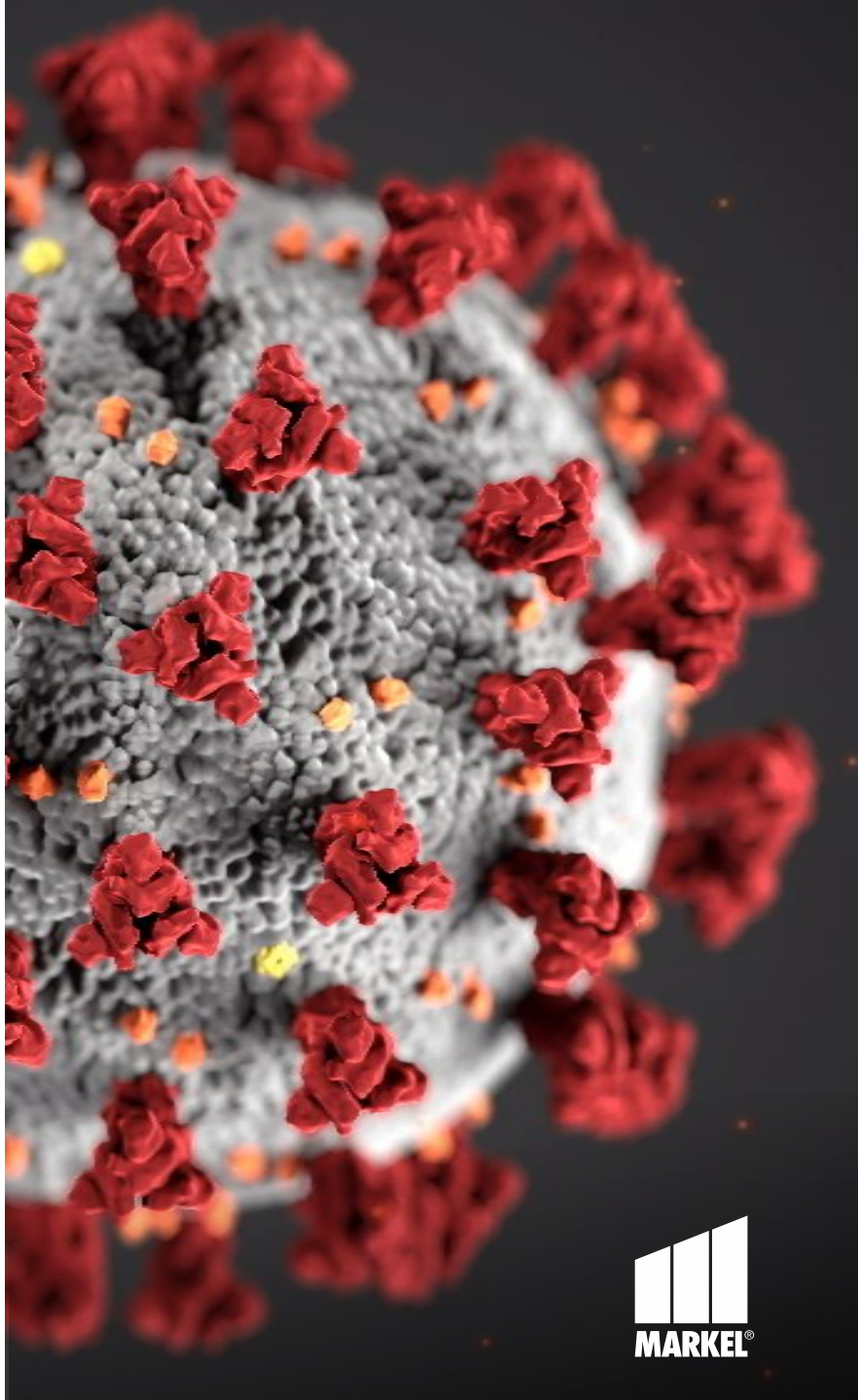


Absicherung des heimischen Arbeitsplatzes

Tipps für das Arbeiten im Home Office

- Verwenden Sie eine aktuelle Antivirensoftware mit Phishing-Schutz
- Vertrauen Sie keinem E-Mail-Absender, den Sie nicht kennen
- Geben Sie niemals Login-Daten preis
- Machen Sie regelmäßig Backups auf externen Datenträgern, die vom System getrennt werden können
- Sicherheitscheck auf den eingerichteten Remotesystemen
- Nach dem Home Office:

  „Quarantäne" für die verwendeten IT-Systeme



Ransomware, Meltdown und Spectre

Gefahr für die Wirtschaft

Ransomware

Meltdown und Spectre

- Anstieg von internationalen Attacken von Malware im 2017 um 500 Prozent im Vergleich zum Vorjahr
- In Deutschland wurde ein Anstieg von 900 Prozent gemessen. Jedes achte Unternehmen war 2016 Opfer eines Cyberangriffs
- Im Jahr 2018 Betrug die Anzahl an Cyberangriffen weltweit 116,5 Mio. €
- Der gesamte Schaden in diesem Bereich beläuft sich auf **55 Mrd. €**

Internet of Things (IoT)

Das Internet der Dinge

- Cyberrisiken die von neuen IoT-Geräten ausgehen, werden noch immer stark vernachlässigt
- Vernetzte TV-Geräte, Wearables und IP-Kameras sind meist ungenügend gesichert
- Unternehmen sind sich oft der Gefahr dieser Systeme nicht bewusst

Je mehr Geräte miteinander vernetzt werden, desto mehr steigt die Gefahr durch Cyberangriffe.

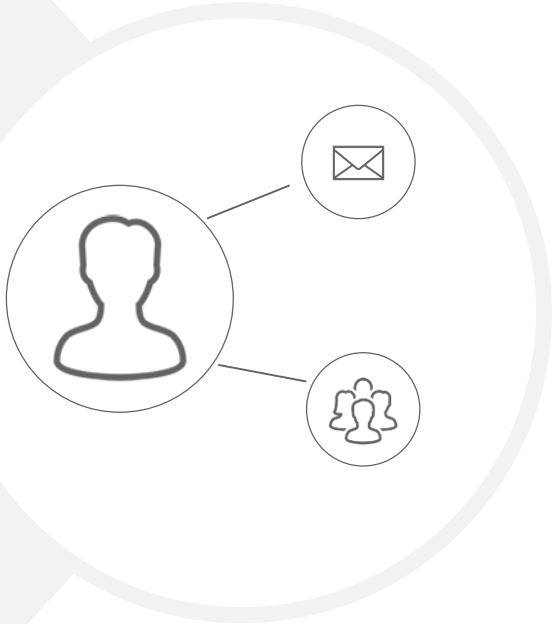
02 Die Schwachstelle Mensch

Social Engineering umgeht alle Technologien einschließlich Firewalls.

*Kevin Mitnick, ehemaliger Hacker und CEO von Defensive Thinking

Social Engineering

Ausnutzen von Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität

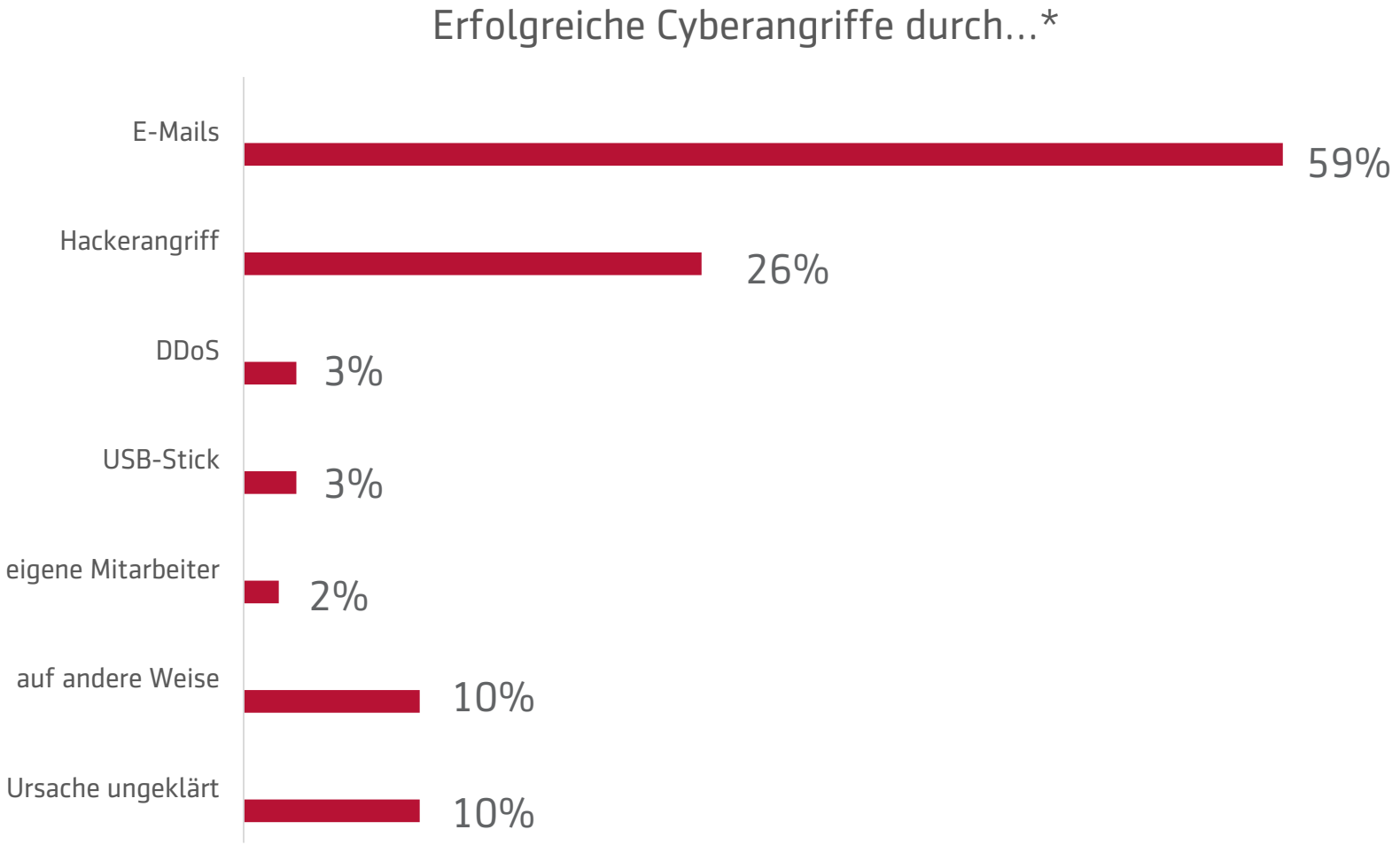


Arten von Social Engineering

- Phishing
- Pretexting
- Spear Phishing
- Vishing
- Hunting
- Farming
- Fake President
- Baiting
- E-Mail-Hacking
- Kontakt-Spamming

Social Engineering

Die Einfallstore



*Mehrfachnennung möglich

*Quelle: GDV Forsa-Befragung Frühjahr 2018

Fake President – CEO Fraud

So funktioniert‘s

Der Beginn

Angreifer sehen, ob sie ihre Domäne fälschen und sich als der CEO (oder andere wichtige Personen) ausgeben können

Der Betrug

Gefälschte E-Mails werden an „risikoreiche“ Mitarbeiter gesendet

Die Antwort

Mitarbeiter erhält die E-Mail und handelt ohne die Quelle zu hinterfragen

Der Schaden

Hacker erhalten Zugang zu dem, was sie gesucht haben

Die wichtigsten Punkte: Geheimhaltung, Dringlichkeit, ...

Fake President – CEO Fraud

Prominente Fälle

- September 2014, Medidata (Softwarefirma) Schadenhöhe 4,1 Mio. €
- November 2015, Hofpfisterei, Schadenhöhe 1,9 Mio. €
- Januar 2016, FACC (Luftfahrttechnik) Schadenhöhe 50 Mio. €
- August 2016, Leoni (Autozulieferer) Schadenhöhe 40 Mio. €
- 2016 – 2017 Facebook und Google, Gesamtschaden 100 Mio. €

Nach Angaben des FBI summieren sich die **weltweiten Schäden auf 2,8 Milliarden €**.

Fake President – CEO Fraud

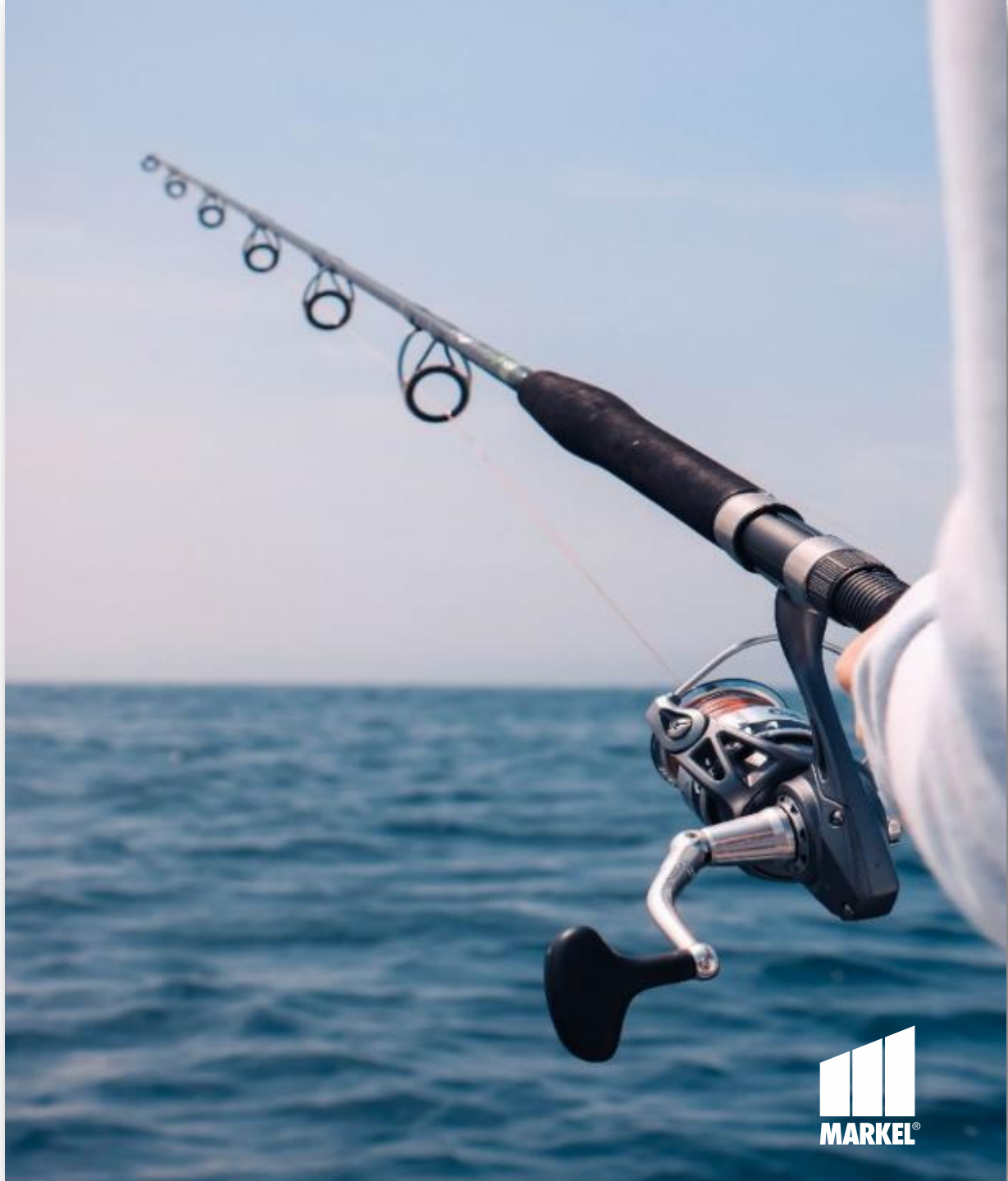
Varianten

Payment Diversion Fraud	Anwalt	IT- Mitarbeiter	Phantomfrachtführer
Betrüger geben sich als Geschäftspartner oder Lieferant aus. Mittels gefälschter Mitteilungen bringen sie das Unternehmen dazu, Geld für Waren oder Dienstleistungen auf andere Konten zu überweisen.	Die Opfer werden aufgefordert Unterlagen zu unterschreiben oder geheime Informationen Preiszugeben.	Ein Betrüger gibt sich als Mitarbeiter der IT-Abteilung aus um an Passwörter zu kommen.	Betrüger geben sich als Frachtführer aus und stehlen ganze LKW Ladungen. Hierzu werden auf Lieferantenbörsen echte Aufträge angenommen.

Phishing

Phishing ist der älteste Trick im großen Buch des Cyber-Betrugs, aber immer noch einer der erfolgreichsten.

- Cyberkriminelle probieren eine ganze Reihe von Methoden aus, um Informationen zu erhalten.
- Die Kriminellen zielen hierbei auf Online-Banking Daten oder einem anderen Online-Account.
- Hierbei wird darauf gebaut, dass Nutzer angstbasierte Entscheidungen treffen – direkt aus dem Bauch heraus, anstatt einen Augenblick nachzudenken.



Phishing

Von: Amazon.de >

Details

Sperrung Ihres Amazon.de Kontos!

29. April 2016 um 02:13

amazon.de

Ihr Amazon.de | Angebote | Alle Kategorien

Guten Tag [redacted],

Ihre Sicherheit ist uns wichtig, daher findet regelmäßig eine Überprüfung der Accounts unserer Kunden statt.

Unser System konnte bei Ihrem Kundenkonto einige unregelmäßige Aktivitäten feststellen.
Ihr Kundenkonto wurde somit automatisch gesperrt, um weitere Risiken zu vermeiden.
Um Ihr Kundenkonto wieder zu entsperren, klicken Sie bitte auf den unten aufgeführten Link, und folgen Sie den weiteren Anweisungen im Formular.

Während des Vorgangs entstehen keine weiteren Kosten für Sie. Folgend sind die geänderte Liefer- und Rechnungsadresse aufgelistet. Bitte entschuldigen Sie aufkommende Unannehmlichkeiten.

› Klicken Sie hier um Ihre Daten zu bestätigen

Baiting (Ködern)

Beim Baiting wird die Neugier des Menschen ausgenutzt.

- Der Cyberkriminelle lässt ein Gerät wie z. B. einen USB-Stick, der mit Schadsoftware infiziert ist, irgendwo an einem öffentlichen Ort liegen.
- Irgendjemand wird das Gerät finden und es in seinen Computer einstecken, um zu sehen, was darauf gespeichert ist.

Spear Phishing

Spear Phishing ist eine komplexere Variante von Phishing.

- Die Kriminellen wählen eine Zielperson innerhalb eines Unternehmens und recherchieren ihr Opfer über Internetsuchen und Social-Media-Profile, um persönliche Informationen und Interessen zu erfahren.
- Sobald die Angreifer ein Gespür für die Zielperson haben, werden scheinbar relevante E-Mails verschickt, um das Opfer zum Klicken auf einen Link, hinter dem sich eine Schadsoftware verbirgt, oder zum Download einer bösartigen Datei zu verleiten.

Vishing

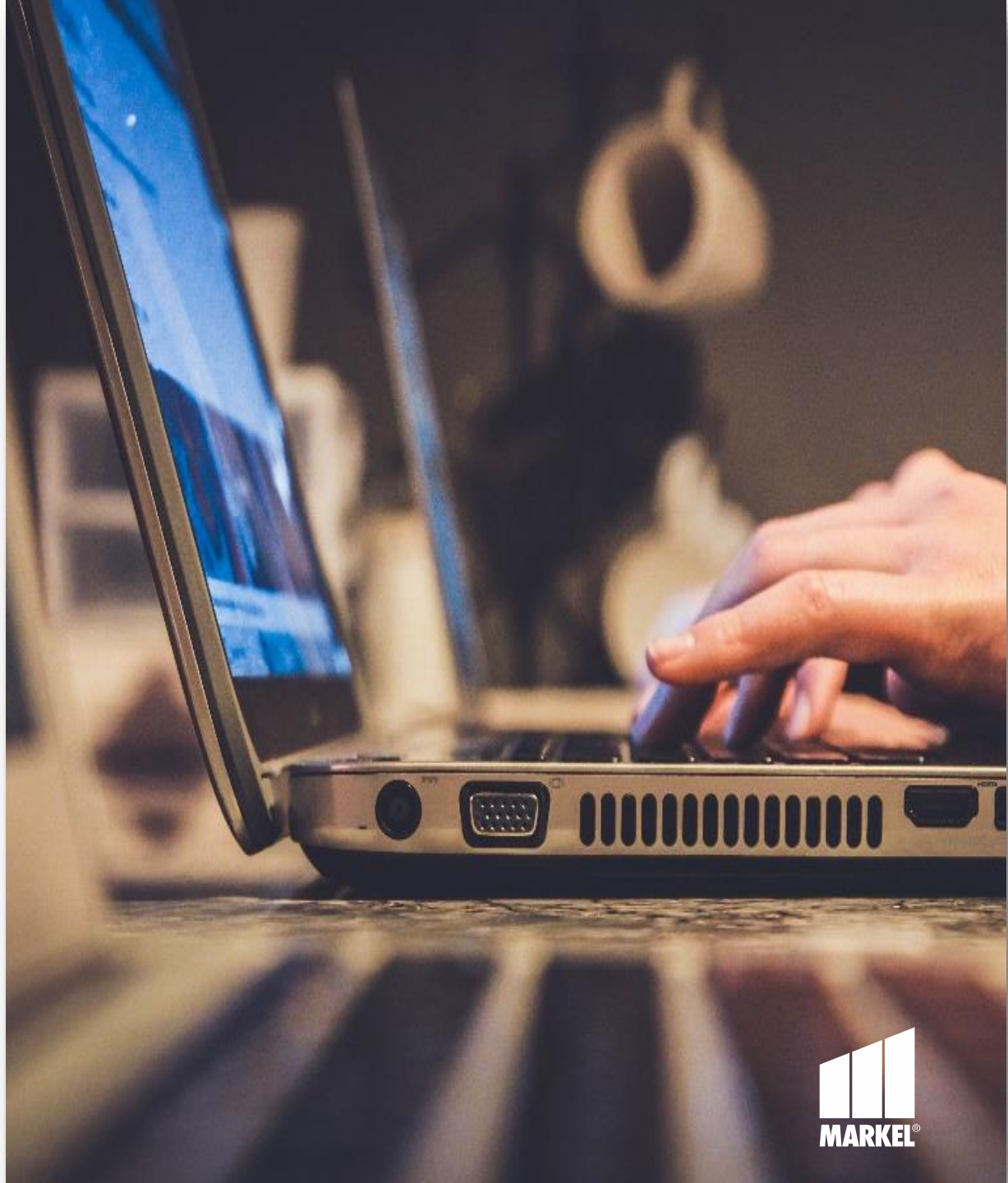
Der Kriminelle ruft einen Mitarbeiter eines Unternehmens an und gibt sich als eine Vertrauensperson aus.

- Er stellt sich als Vertreter der Bank oder einer anderen Firma vor, mit der Geschäftsbeziehungen bestehen.
- Dann versucht er, Informationen von seinen Opfern abzufischen, indem er sich als Kollege ausgibt, der sein Passwort verloren hat und bittet um das Passwort des Mitarbeiters. Er stellt eine Reihe von Fragen, um die Identität zu bestätigen.

E-Mail-Hacking und Kontakt-Spamming

Kriminelle versenden Emails mit vermeintlich interessanten Inhalt für das Opfer.

- „Sieh dir mal diese Website an, die finde ich absolut cool“.
- Nachdem das Opfer sich auf der Website eingeloggt hat, werden E-Mail und Passwort gestohlen.
- Mit diesen Informationen übernehmen die Kriminellen die Kontrolle über den Account und versenden Spam-Mails an die Kontakte.



Pretexting

Kriminelle erfinden eine rührselige Geschichte (man sitzt im Ausland fest und benötigt Geld, Afrikanischer Prinz benötigt 5.000 € um König zu werden).

- Dem Opfer wird versprochen nach der Zahlung des Betrages ein vielfaches davon zurückzuerhalten.
- Hierbei Zielen die Kriminellen auf die Hilfsbereitschaft und Gier des Opfers ab.

Maßnahmen zur Vorbeugung

Was kann das Unternehmen tun?

1. **Prozesse überdenken**
   Prozesse, Richtlinien und IT Systeme im Unternehmen auf Schwachstellen überprüfen und gegebenenfalls anpassen

2. **Notfallkonzept**
   Erstellung eines Notfallkonzeptes für den Fall das ein Betrug tatsächlich stattgefunden hat

3. **Mitarbeiter**
   Mitarbeiter sensibilisieren und anhand Trainings auf Betrugsversuche vorbereiten

4. **Vorsicht**
   Soziale Netzwerke bieten Kriminellen nützliche Informationen

5. **Gesundes Misstrauen**
   Identität des Anrufers/ Versenders genau feststellen

6. **Prüfen**
   E-Mail Versender Adresse genau prüfen. Unbekannte Dateien und Dateiformate nicht öffnen

03 Cyber Cysmo-Report

Cyber Cysmo-Report

Ableitung von präventiven Maßnahmen für die Sicherheit Ihres Kunden

Systemcheck

DDOS-Stabilität

DNS-Configuration

Mail-Configuration

Privatsphäre und Reputation

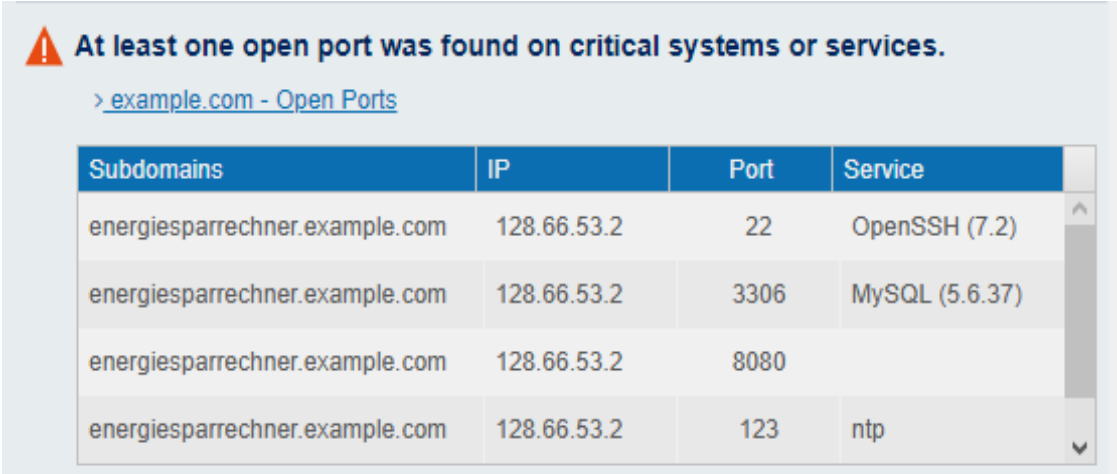
Darknet

Tipp: Der Cyber Cysmo-Report liefert Ihnen interessante Punkte zur Sicherheit Ihres Kunden.

Systemcheck

Wonach wird gesucht?

- Hostnamen die auf interne Systeme hinweisen oder die verwendete Software verraten
- Services die nicht von extern erreichbar sein sollten (fileserver, databases)
- Unübliche Konfigurationen (z. B. FTP-server auf dem Mailserver)
- Login´s (speziel backend logins)
- Server welche bereits infiziert sind



At least one open port was found on critical systems or services.

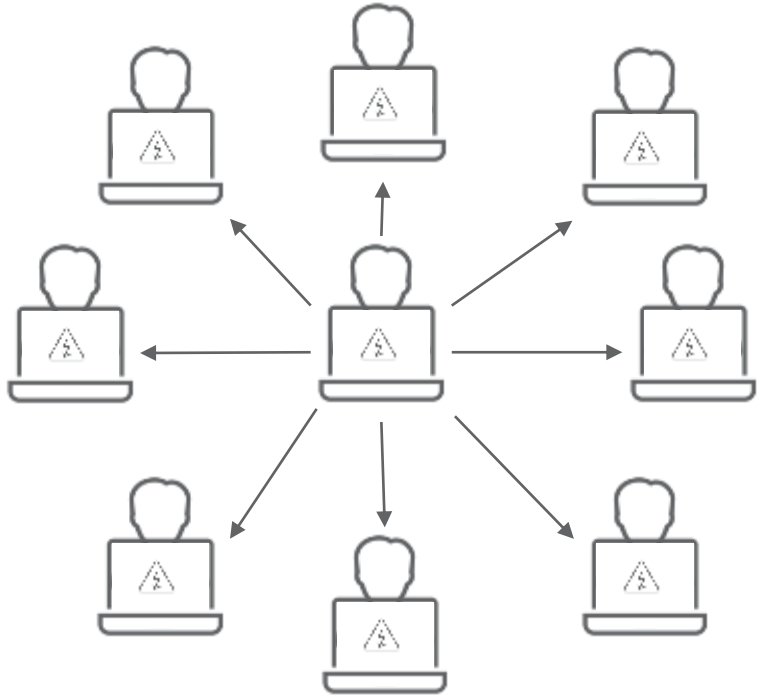
› example.com - Open Ports

Subdomains	IP	Port	Service
energiesparrechner.example.com	128.66.53.2	22	OpenSSH (7.2)
energiesparrechner.example.com	128.66.53.2	3306	MySQL (5.6.37)
energiesparrechner.example.com	128.66.53.2	8080	
energiesparrechner.example.com	128.66.53.2	123	ntp

DDOS-Stabilität

Wie sicher sind die Systeme vor DDOS-Attacken?

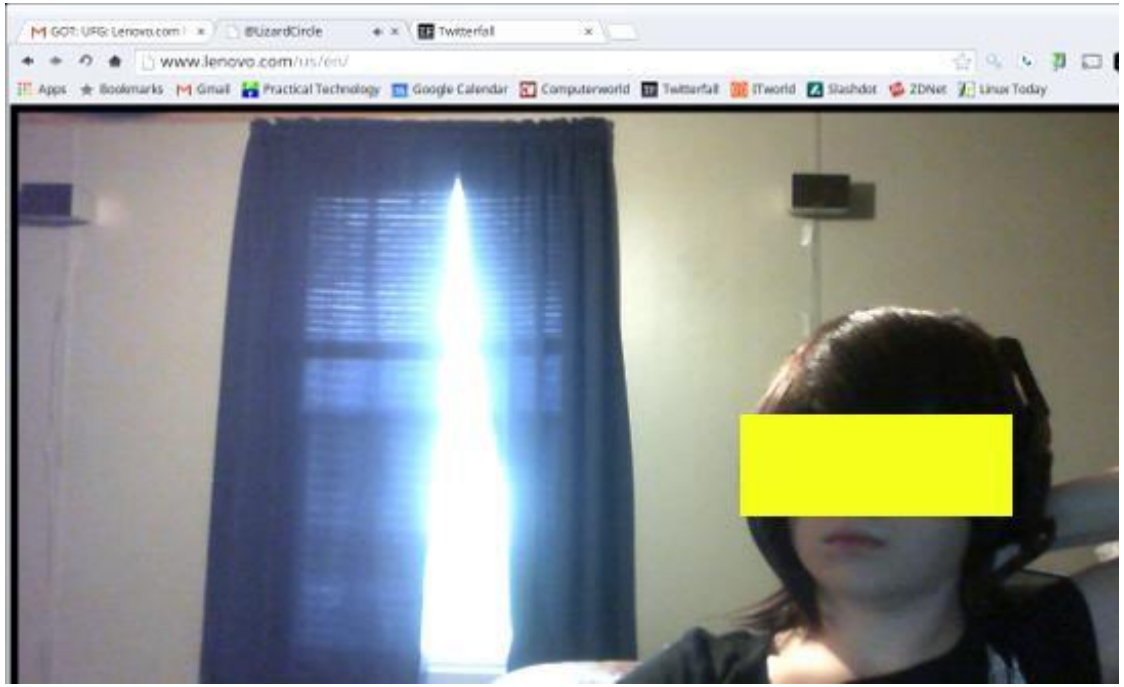
- Die Abwehr von (D)DOS Attacken ist ein Materialkampf.
- Man kann unabsichtlich Teil einer DDOS Attacke werden.
- DDOS Attacken sind Preiswert.



DNS-Configuration

Domain Diebstahl

- Registrierungsänderung ohne Einwilligung des Inhabers.
- Ziele: Bloßstellen, Phishing von Kundendaten, Verbreitung von Malware, Unterbrechung des Geschäftsbetriebes.
- Cyber-Rating prüft u.a. die Einstellungen zur Domain Registrierung



https://www.zdnet.com/article/lenovo-website-hacked

Mail-Config

Spoofing

From: Angela Merkel
<a.merkel@bundesregierung.de>

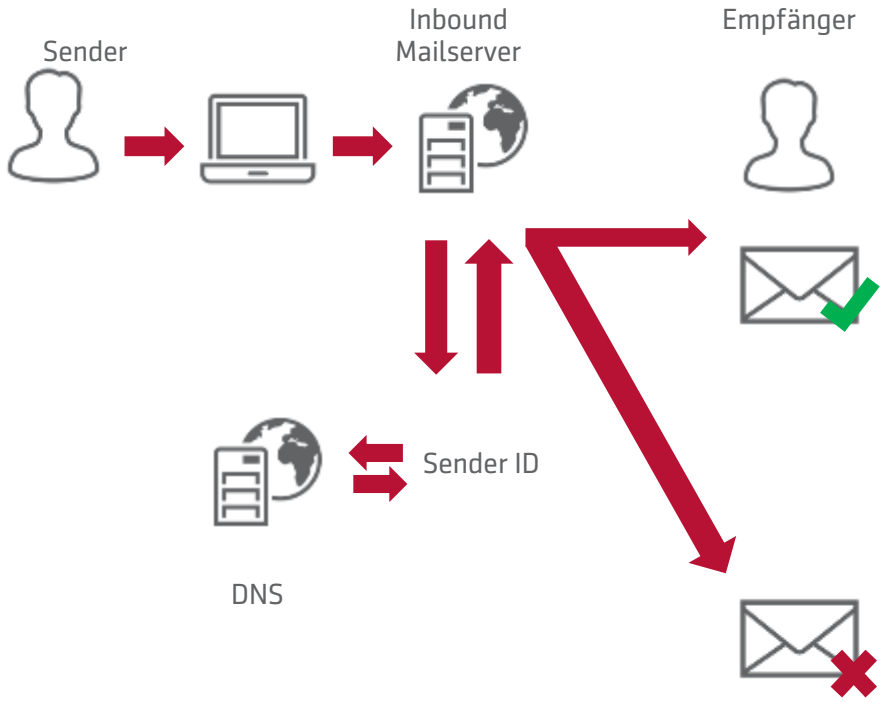
To: Stephan Lindner
<Stephan Lindner@markel.de>

Subject: Your country needs you, click this link!

Spoofing wird für Social Engineering Attacken und zur Verbreitung von Malware verwendet.

Kriminelle kaufen E-Mail Metadaten im Darknet und verwenden bekannte Sender-Empfänger Adressen.

Zur Vermeidung von Spoofing sollten Methoden wie SPF und DKIM verwendet werden – Das Rating prüft dies.



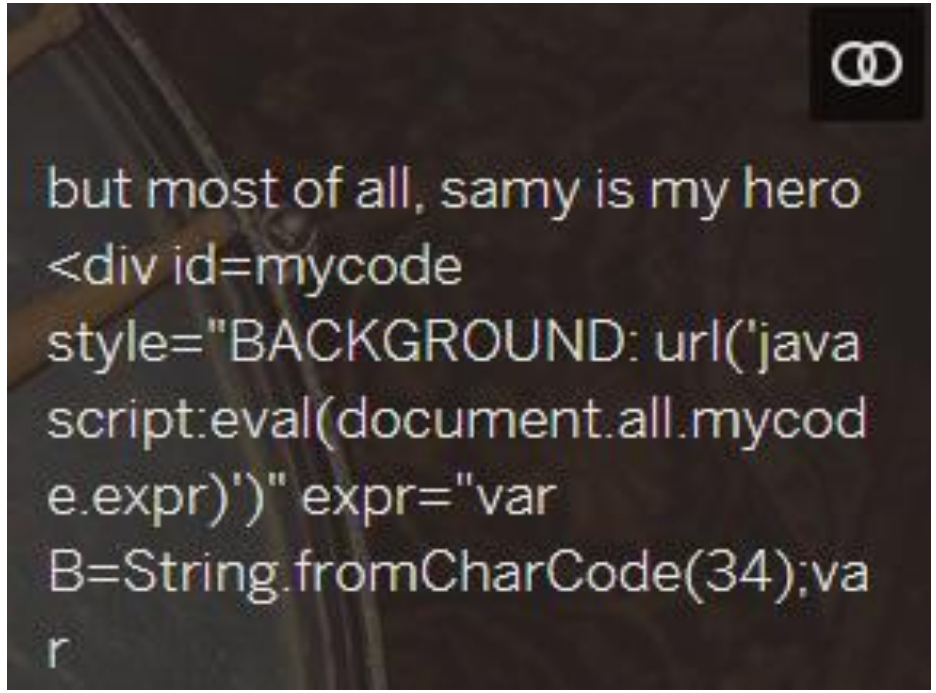
Privatsphäre und Reputation

Ein Problem von 2009 bis heute

Berühmtes Beispiel: 2005 infizierte der XXS-Wurm “Samy” mehr als 1 Million User auf MySpace in weniger als 20 Stunden – Das macht ihn zum am schnellsten verbreiteten Virus aller Zeiten.

Zu dieser Zeit validierte MySpace den Input der User nicht.

Heutzutage gibt es Sicherheitseinstellungen die dies vermeiden können - Einige Webentwickler ignorieren dies jedoch.



https://en.wikipedia.org/wiki/File:SamyIsMyHero.png

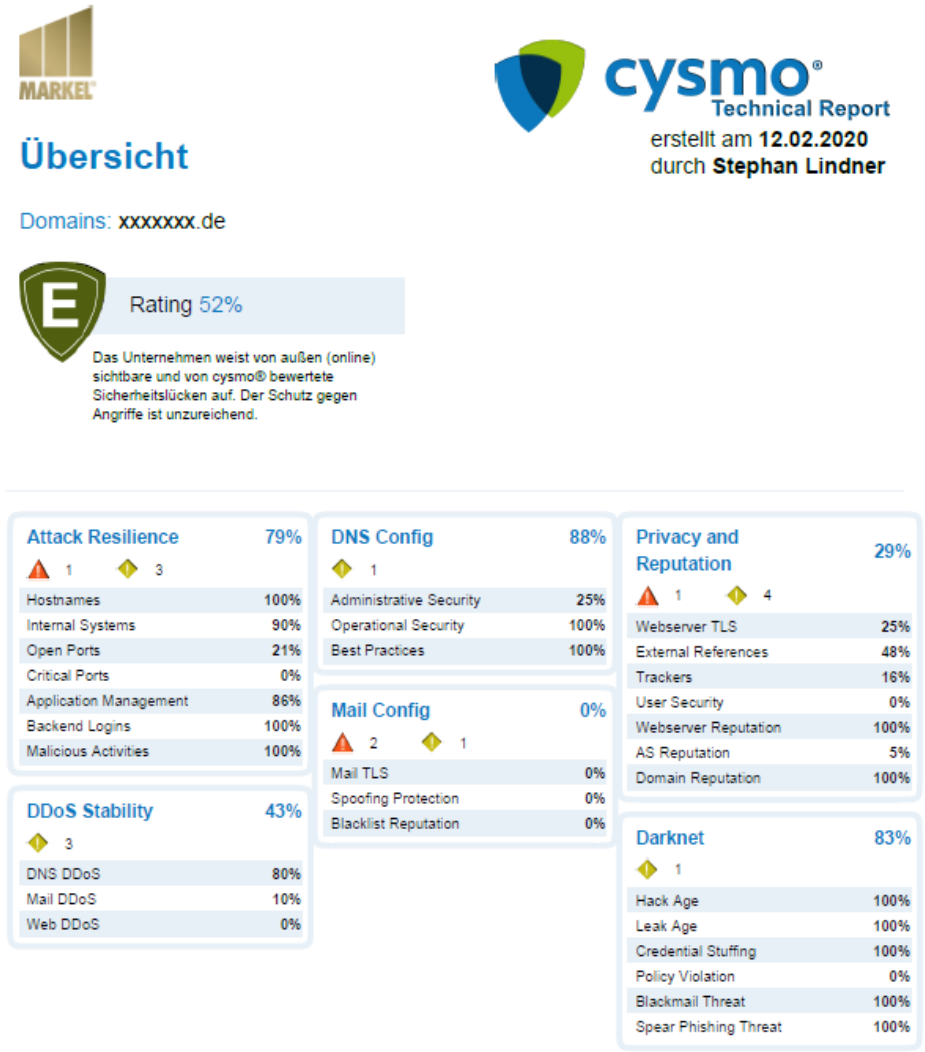
Darknet

Cysmo erkennt Risiken aus Datenmissbrauch

- Übersicht: Ist das Unternehmen direkt oder indirekt betroffen
- Passwortsicherheit: Wie hoch ist die Wahrscheinlichkeit, dass Passwörter Zugang zu Unternehmensnetzwerken erlauben
- Spearphishing: Wie viele persönliche Informationen können für Social Engineering Attacken verwendet werden
- Verstöße gegen Firmenrichtlinien: Verwenden Mitarbeiter Firmenaccounts für Private Zwecke
- Illegale Handlungen: Werden E-Mailadressen zu illegalen Zwecken verwendet

Gefahren aufdecken – Kunden aufwecken

Cyber-Rating



cysmo® Technical Report
erstellt am **12.02.2020**
durch **Stephan Lindner**

Übersicht

Domains: **xxxxxxx**.de

Rating 52%

Das Unternehmen weist von außen (online) sichtbare und von cysmo® bewertete Sicherheitslücken auf. Der Schutz gegen Angriffe ist unzureichend.

Attack Resilience 79%

1 3

Hostnames	100%
Internal Systems	90%
Open Ports	21%
Critical Ports	0%
Application Management	86%
Backend Logins	100%
Malicious Activities	100%

DDoS Stability 43%

3

DNS DDoS	80%
Mail DDoS	10%
Web DDoS	0%

DNS Config 88%

1

Administrative Security	25%
Operational Security	100%
Best Practices	100%

Mail Config 0%

2 1

Mail TLS	0%
Spoofing Protection	0%
Blacklist Reputation	0%

Privacy and Reputation 29%

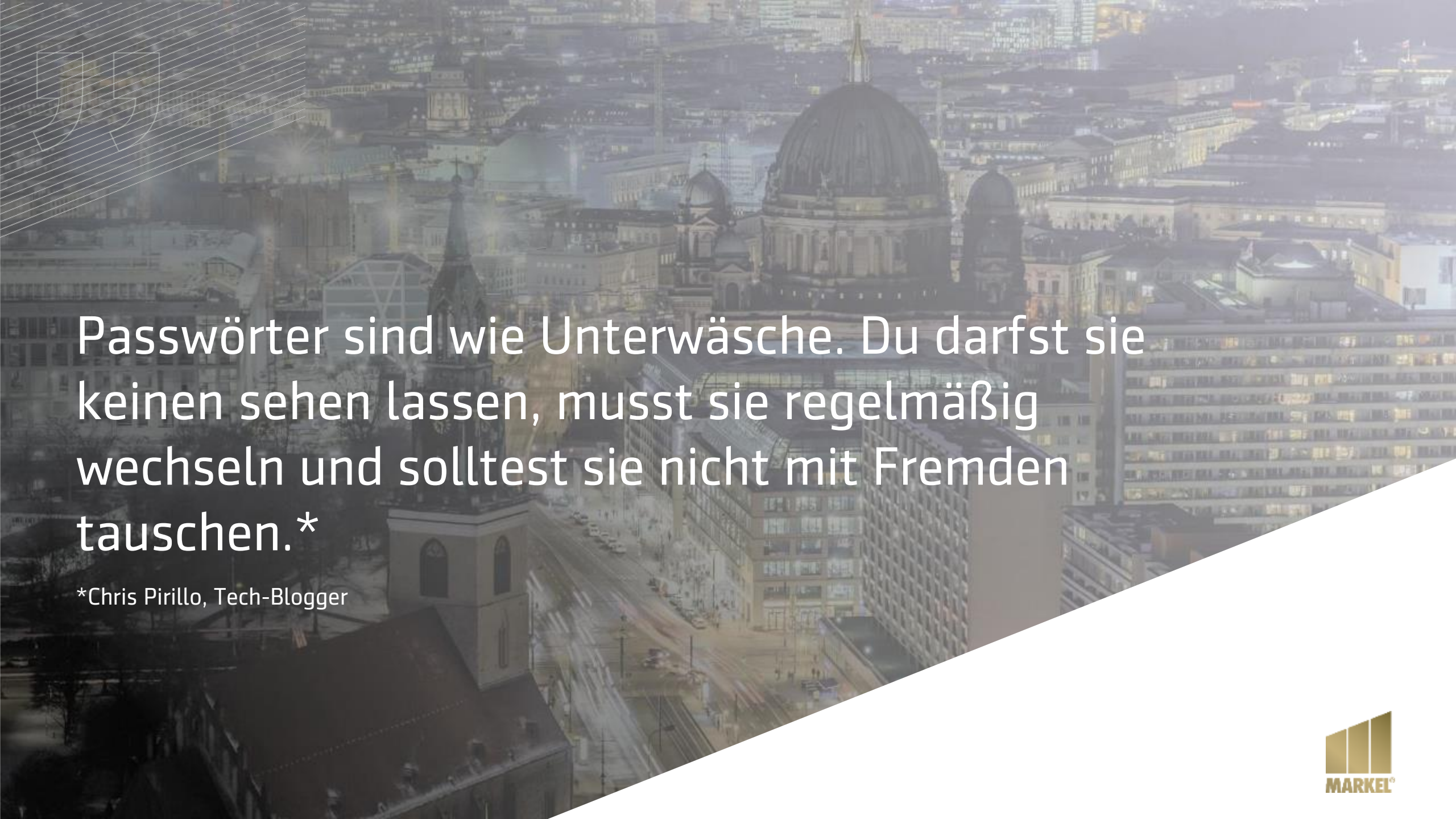
1 4

Webserver TLS	25%
External References	48%
Trackers	16%
User Security	0%
Webserver Reputation	100%
AS Reputation	5%
Domain Reputation	100%

Darknet 83%

1

Hack Age	100%
Leak Age	100%
Credential Stuffing	100%
Policy Violation	0%
Blackmail Threat	100%
Spear Phishing Threat	100%


Passwörter sind wie Unterwäsche. Du darfst sie keinen sehen lassen, musst sie regelmäßig wechseln und solltest sie nicht mit Fremden tauschen.*
*Chris Pirillo, Tech-Blogger
MARKEL

04 Die Cyber-Versicherung
Der Schadenfall

Schadenbeispiel I

Online Erpressung mittels Ransomware

Die IT-Systeme einer mittelständischen Zahnarztpraxis werden am 17.01.2019 durch eine Ransomware-Attacke „lahm“ gelegt. Der Hacker platzierte eine Text-Datei mit der Forderung einer gewissen Summe zur Entschlüsselung der Systeme in jeden Ordner.

Nach Absprache mit der Polizei wird auf die Forderung nicht eingegangen.

Der interne Datenschutzbeauftragte versuchte zunächst selbst, den Schaden zu beheben, schaffte dies aber nicht auf anhieb. Somit kam es zu einer Beeinträchtigung einiger PCs, welcher bis zum 28.01.2019 andauerte. Nach der Meldung des Schadens am 28.01.2019 wurde umgehende der IT-Support eingeschaltet.

Nach Prüfung der Sachlage stellte sich heraus, dass der Trojaner durch das Öffnen einer Bewerbung, welche über eine E-Mail an den Versicherungsnehmer gelangt ist, auf die IT-Systeme gelangt sind.

Zur Regulierung des Schadens wurden dem Versicherungsnehmer von uns die vom IT-Support in Rechnung gestellten Kosten in Höhe von 5.145 € zur Wiederherstellung der Daten und des Beseitigen des Virus erstattet.

Schadenbeispiel II

Betriebsunterbrechung

Am 19.01.2020 wurden die Daten auf dem Server einer Rechtsanwaltkanzlei durch eine Ransomware namens LockBit verschlüsselt. Zunächst war nicht klar über welchen Weg der Hacker Zugriff auf das Systems des Versicherungsnehmers erlangte und lies sich auch nicht mehr rekonstruieren.

Nachdem der Versicherungsnehmer sich seines Schadens/Risikos bewusst war, kontaktierte er umgehend den externen IT-Support-Dienstleister, welcher sofort zur Stelle war.

Der Versicherer beglich die Rechnung des IT-Dienstleisters zur Entschlüsselung der Daten und die Wiederherstellung des Backups.

Schadenbeispiel II

Bearbeitung durch den IT-Support

Schadenseingang	19.01	Erstgespräch über das weitere Vorgehen, wie am nächsten Tag erstmal alle Systeme gegen Wiederbefall abgesichert werden sollen
Virenscanung + Problembehebung	20.01	VPN Umgebung gesichert und gescannt auf Viren, Hilfestellungen für den lokalen ITler geleistet (Backup, weiteres Vorgehen und Wiederherstellung)
Wiederherstllung der Backups	21.01	Backupumsetzungen des Itlers, zwischenzeitlich kurze Telefonate um diverse Rückfragen zu besprechen für die Best-Practice Umsetzung der Systeme. Rückfragen bei Softwarehersteller um diverse Virenfunde zu klären
Optimierung der IT-Systeme	22.01	Telefonkonferenz mit Kunden und Techniker, Abschlussgespräch und unsere Checkliste für die Optimierung der Umgebung wurde rausgesendet.

05 Markel Pro Cyber **Deckungshighlights**

Markel Pro Cyber

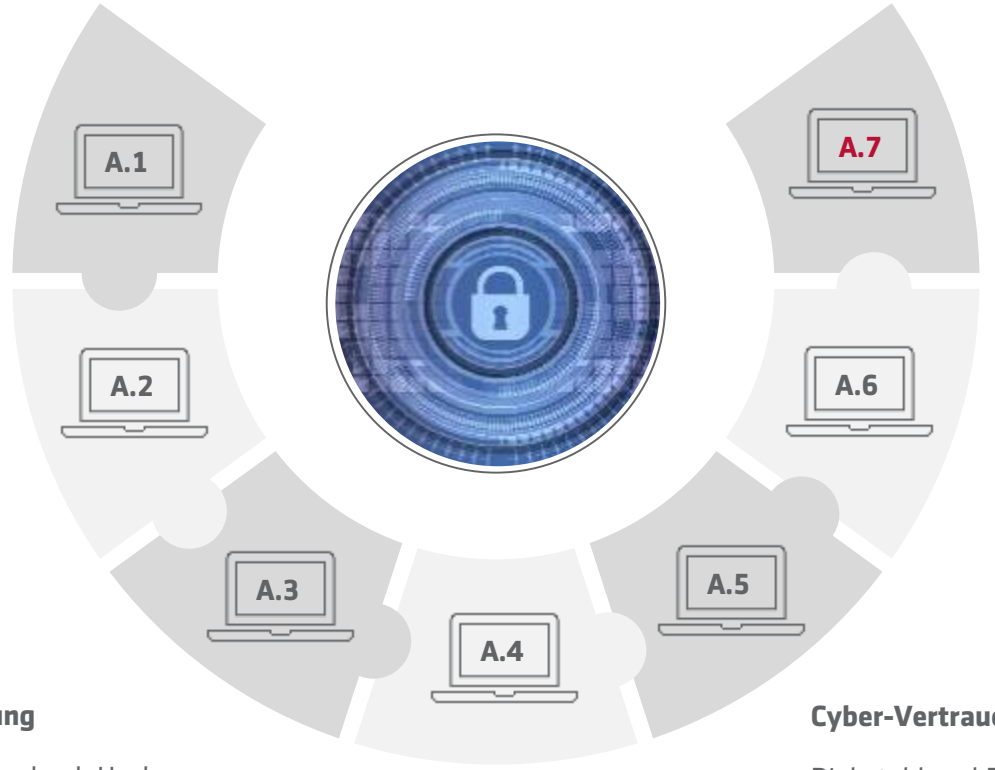
Modularer Versicherungsschutz mit **frei wählbaren** Deckungsinhalten

Cyber Daten- und Eigenschäden

Wiederherstellung der Hard- und Software

Cyber Betriebsunterbrechung

Ertragsausfall für den Zeitraum der versicherten Betriebsunterbrechung



Cyber-Prävention Premium

Online-Präventionsplattform von Perseus

Cyber-Haftpflicht

Haftpflichtansprüche seitens Dritte aus den Bereichen des Datenschutzes (EU-DSGVO, BDSG)

Cyber-Erpressung

Geldforderungen durch Hacker gegenüber den Versicherten

Cyber-Zahlungsmittel

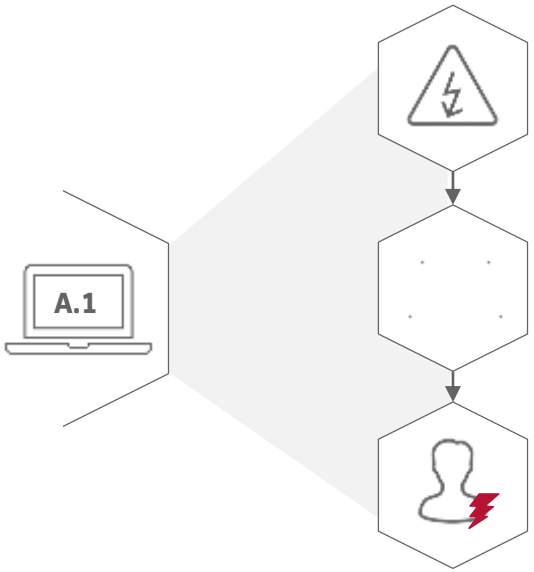
Forderungen der Kreditkartenindustrie wie z.B. Banken oder PayPal

Cyber-Vertrauensschaden

Diebstahl und Betrug durch mitversicherte Personen oder Dritte sowie Fake-President, Social-Engenierung

Highlights A.1

Cyber- und Dateneigenschäden



Beschädigung, Zerstörung, Veränderung, Blockierung oder der Missbrauch

der IT-Systeme (auch mobile Geräte), der Programme und der elektronischen Daten des Versicherten

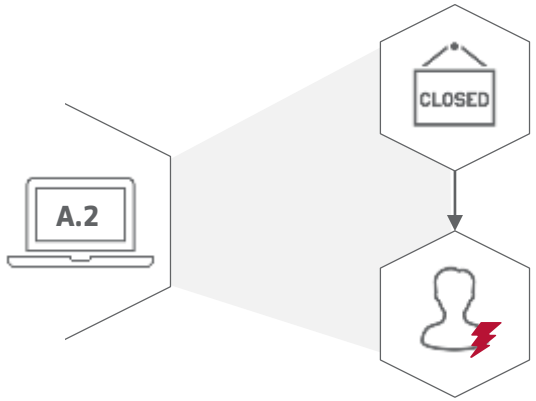
Durch einen Hacker-Einbruch, einer DDOS Attacke oder einer Infektion durch Schadsoftware

Ebenfalls besteht Versicherungsschutz bei einem Angriff durch eine mitversicherte Person bei Gelegenheit einer dienstlichen Tätigkeit (**Innentäter**) und bei **Bedienfehlern** der Versicherten.

Im Baustein A.1. ist die Assistance Leistung „Perseus Basis“ beinhaltet!

Highlights A.2

Cyber-Betriebsunterbrechung



Betriebsunterbrechungsschaden durch: Unterbrechung oder Beeinträchtigung des versicherten Geschäftsbetriebs infolge

Hacker-Einbruchs; eines unbefugten Angriffs oder mit dem Ziel, die IT-Systeme der Versicherten zu unterbrechen (DoS – Denial of Service); Infektion durch Schadsoftware

Versicherungsschutz besteht auch bei Nutzung von Cloud-Diensten ohne Zuschlag!

Highlights A.3

Cyber-Erpressung

Geld- oder Warenforderung durch Dritte

im Zusammenhang mit angedrohter oder bereits erfolgter Beschädigung, Zerstörung, Veränderung, Blockierung oder den Missbrauch

der IT-Systeme, der Programme und der elektronischen Daten des Versicherten (insbesondere der Auftragsdaten, Kundendaten, Personendaten)

Versicherungsschutz wird auch gewährt, wenn der Erpresser eine mitversicherte Person ist!

Highlights A.4

Cyber-Zahlungsmittel

Verstöße gegen…

Vertragspflichten von Kreditkartenverarbeitungsvereinbarungen

Vereinbarungen im Zusammenhang mit anderen Bezahlsystemen wie beispielsweise Bankkarten (EC-Karten)

Vereinbarungen mit Zahlungsprozessoren (z.B. Paypal)

Markel ersetzt nicht nur den entstandenen Vermögensschaden sondern auch alle angemessenen und notwendigen Kosten für die Beauftragung eines Dienstleisters zur Prüfung und Benachrichtigung für einen Zeitraum von maximal 12 Monaten, wenn Anhaltspunkte für den Missbrauch personenbezogener Daten
bestehen (Monitoring).

Highlights A.5

Cyber- und Dateneigenschäden

Vertrauensschäden durch eigene Mitarbeiter

(Betrug, Urkundenfälschung, Unterschlagung, Diebstahl)

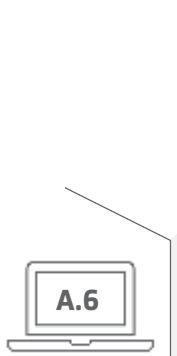
Vertrauensschäden durch Dritte

(Betrug, Urkundenfälschung, Unterschlagung, Diebstahl von Firmengeldern wie z.B. Phishing)

Fake President und andere Social Engineering Schäden gelten auch versichert!

Highlights A.6

Cyber-Haftpflicht



- Verstöße gegen die Cyber-Sicherheit (Weitergabe von Schadsoftware)
- Verstöße gegen den Datenschutz
- Cyber-Spionage/ Verstöße gegen Geheimhaltungspflichten
- Vertragsstrafen bei Verletzung von Geheimhaltungspflichten
- Verstöße gegen Namens- und Persönlichkeitsrechte
- Verstöße durch Werbung und Marketing
- Straf- oder Bußgelder gelten mitversichert (sofern gesetzlich erlaubt)
- Freistellung externer Datenverarbeiter
- Straf- und Ordnungswidrigkeiten-Rechtsschutz

Cyber-Prävention

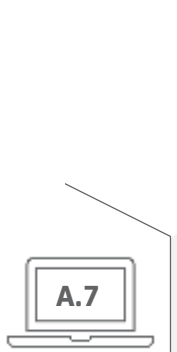
Cyber-Prävention Basis (prämienneutral enthalten)

perseus.

- ✓ Einmalige IT-Sicherheitsprüfung
- ✓ Online-Training Cybersicherheit & Datenschutz für maximal 3 Mitarbeiter
- ✓ Einmaliger Phishing-Test
- ✓ Browser-Check
- ✓ Passwort Generator
- ✓ Checklisten

Highlights A.7

Cyber-Prävention (NEU)

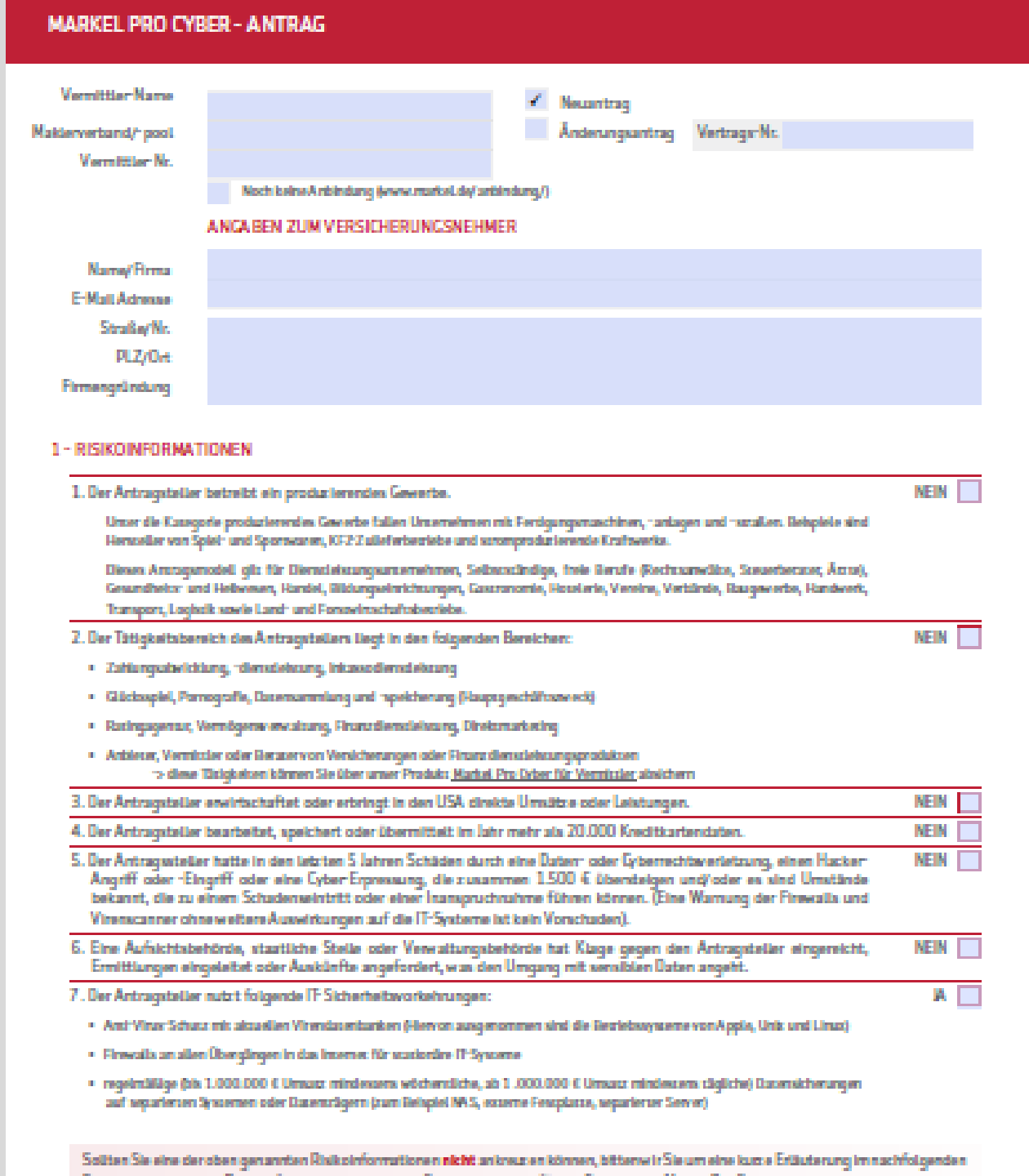


- Online-Training für Cybersicherheit und Datenschutz für eine unbegrenzte Anzahl von Mitarbeitern
- Laufende Phishing-Test
- Online-Konto-Check
- E-Mail-Scanner
- Systemische und gezielte Aktivierung der Mitarbeiter zur Nutzung der Tools
- Angriffsalarm
- Reportingbereich mit Online-Training-Statistik und Cyber-Sicherheits-Scores
- Checkliste zum Verhalten im Cyber-Fall
- Passwort-Generator und Browser-Check

06 Ihre Vertriebsunterstützung

Das Antragsmodell der Cyberversicherung

- ✓ **Selbstrechnend** & **intelligent**
- ✓ Häkchen setzen – und der **Kunde ist versichert**
- ✓ **VVG konform** und **haftungssicher**



MARKEL PRO CYBER - ANTRAG

Vermittler-Name
Maklerverband/-pool
Vermittler-Nr.

☑ Neuantrag
☐ Änderungsantrag
Vertrags-Nr.

☐ Noch keine Anbindung (www.markel.de/anbindung/)

ANGABEN ZUM VERSICHERUNGSNEHMER

Name/Firma
E-Mail Adresse
Straße/Nr.
PLZ/Ort
Firmengründung

1 - RISIKOINFORMATIONEN

1. Der Antragsteller betreibt ein produzierendes Gewerbe. NEIN ☐

Unter die Kategorie produzierendes Gewerbe fallen Unternehmen mit Fertigungsmaschinen, -anlagen und -straßen. Beispiele sind Hersteller von Spiel- und Sportwaren, KFZ-Zulieferbetriebe und stromproduzierende Kraftwerke.

Diesen Antragsmodell gilt für Dienstleistungsunternehmen, Selbstständige, freie Berufe (Rechtsanwälte, Steuerberater, Ärzte), Gesundheits- und Heilwesen, Handel, Bildungseinrichtungen, Gastronomie, Hotellerie, Vereine, Verbände, Baugewerbe, Handwerk, Transport, Logistik sowie Land- und Forstwirtschaftsbetriebe.

2. Der Tätigkeitsbereich des Antragstellers liegt in den folgenden Bereichen: NEIN ☐

- Zahlungsabwicklung, -dienstleistung, Inkassodienstleistung
- Glücksspiel, Pornografie, Datensammlung und -speicherung (Hauptgeschäftszweck)
- Rating-agentur, Vermögensverwaltung, Finanzdienstleistung, Direktmarketing
- Anbieter, Vermittler oder Betreiber von Versicherungen oder Finanzdienstleistungsprodukten
  -> diese Tätigkeiten können Sie über unser Produkt Markel Pro Cyber für Vermittler absichern

3. Der Antragsteller erwirtschaftet oder erbringt in den USA direkte Umsätze oder Leistungen. NEIN ☐

4. Der Antragsteller bearbeitet, speichert oder übermittelt im Jahr mehr als 20.000 Kreditkartendaten. NEIN ☐

5. Der Antragsteller hatte in den letzten 5 Jahren Schäden durch eine Daten- oder Cybersicherheitsverletzung, einen Hacker-Angriff oder -Eingriff oder eine Cyber-Erpressung, die zusammen 1.500 € übersteigen und/oder es sind Umstände bekannt, die zu einem Schadenseintritt oder einer Inanspruchnahme führen können. (Eine Warnung der Firewalls und Virenscanner ohne weitere Auswirkungen auf die IT-Systeme ist kein Vorschaden). NEIN ☐

6. Eine Aufsichtsbehörde, staatliche Stelle oder Verwaltungsbehörde hat Klage gegen den Antragsteller eingereicht, Ermittlungen eingeleitet oder Auskünfte angefordert, was den Umgang mit sensiblen Daten angeht. NEIN ☐

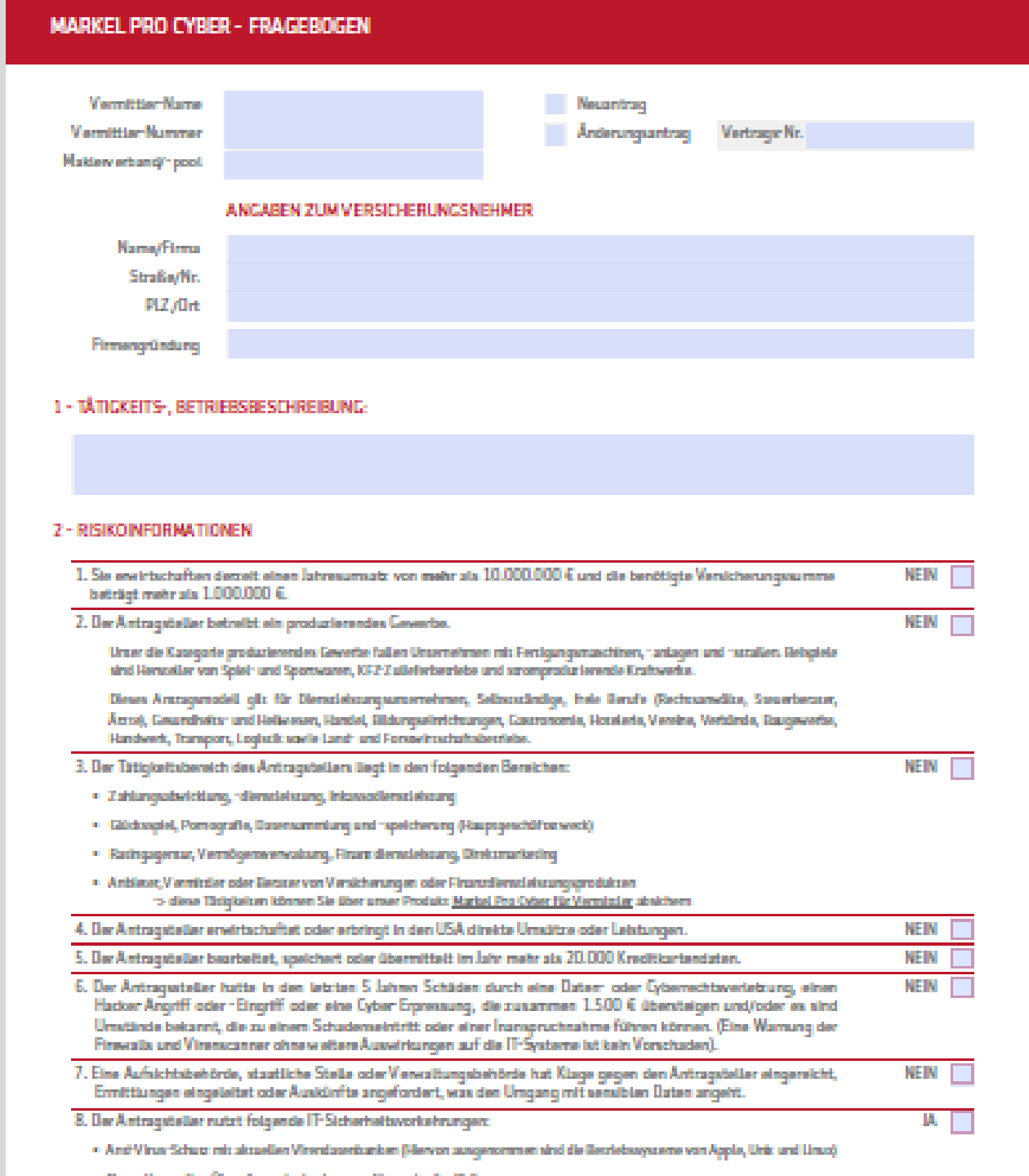
7. Der Antragsteller nutzt folgende IT-Sicherheitsvorkehrungen: JA ☐

- Anti-Virus-Schutz mit aktuellen Virendefinitionen (Hiervon ausgenommen sind die Betriebssysteme von Apple, Unix und Linux)
- Firewalls an allen Übergängen in das Internet für sensible IT-Systeme
- regelmäßige (bis 1.000.000 € Umsatz mindestens wöchentliche, ab 1.000.000 € Umsatz mindestens tägliche) Datensicherungen auf separaten Systemen oder Datenträgern (zum Beispiel NAS, externe Festplatte, separater Server)

Sollten Sie eine der oben genannten Risikoinformationen **nicht** ankreuzen können, bitten wir Sie um eine kurze Erläuterung im nachfolgenden

Der Fragebogen der Cyber-Versicherung

Fragebogen nur nötig bei negativ beantworteten Risikofragen oder höheren Deckungssummen/Umsätzen



MARKEL PRO CYBER - FRAGEBOGEN

Vermittler-Name
Vermittler-Nummer
Maklerverbund/-pool

☐ Neuantrag
☐ Änderungsantrag
Vertrags-Nr.

ANGABEN ZUM VERSICHERUNGSNEHMER

Name/Firma
Straße/Nr.
PLZ/Ort
Firmengründung

1 - TÄTIGKEITS-, BETRIEBSBESCHREIBUNG:

2 - RISIKOINFORMATIONEN

1. Sie erwirtschaften derzeit einen Jahresumsatz von mehr als 10.000.000 € und die benötigte Versicherungssumme beträgt mehr als 1.000.000 €. NEIN ☐

2. Der Antragsteller betreibt ein produzierendes Gewerbe. NEIN ☐

   Unter die Kategorie produzierendes Gewerbe fallen Unternehmen mit Fertigungsmaschinen, -anlagen und -straßen. Beispiele sind Hersteller von Spiel- und Sportwaren, KFZ-Zulieferbetriebe und stromproduzierende Kraftwerke.

   Dieses Antragsmodell gilt für Dienstleistungsunternehmen, Selbstständige, freie Berufe (Rechtsanwälte, Steuerberater, Ärzte), Gesundheits- und Heilwesen, Handel, Bildungseinrichtungen, Gastronomie, Hotellerie, Vereine, Verbände, Baugewerbe, Handwerk, Transport, Logistik sowie Land- und Forstwirtschaftsbetriebe.

3. Der Tätigkeitsbereich des Antragstellers liegt in den folgenden Bereichen: NEIN ☐

   - Zahlungsabwicklung, -dienstleistung, Inkassodienstleistung
   - Glücksspiel, Pornografie, Datensammlung und -speicherung (Hauptgeschäftszweck)
   - Rating-agentur, Vermögensverwaltung, Finanzdienstleistung, Direktmarketing
   - Anbieter, Vermittler oder Berater von Versicherungen oder Finanzdienstleistungsprodukten
     -> diese Tätigkeiten können Sie über unser Produkt Markel Pro Cyber Fin Vermittler abdecken

4. Der Antragsteller erwirtschaftet oder erbringt in den USA direkte Umsätze oder Leistungen. NEIN ☐

5. Der Antragsteller bearbeitet, speichert oder übermittelt im Jahr mehr als 20.000 Kreditkartendaten. NEIN ☐

6. Der Antragsteller hatte in den letzten 5 Jahren Schäden durch eine Daten- oder Cybersicherheitsverletzung, einen Hacker-Angriff oder -Eingriff oder eine Cyber-Erpressung, die zusammen 1.500 € übersteigen und/oder es sind Umstände bekannt, die zu einem Schadenseintritt oder einer Inanspruchnahme führen können. (Eine Warnung der Firewalls und Virenscanner ohne weitere Auswirkungen auf die IT-Systeme ist kein Vorschaden). NEIN ☐

7. Eine Aufsichtsbehörde, staatliche Stelle oder Verwaltungsbehörde hat Klage gegen den Antragsteller eingereicht, Ermittlungen eingeleitet oder Auskünfte angefordert, was den Umgang mit sensiblen Daten angeht. NEIN ☐

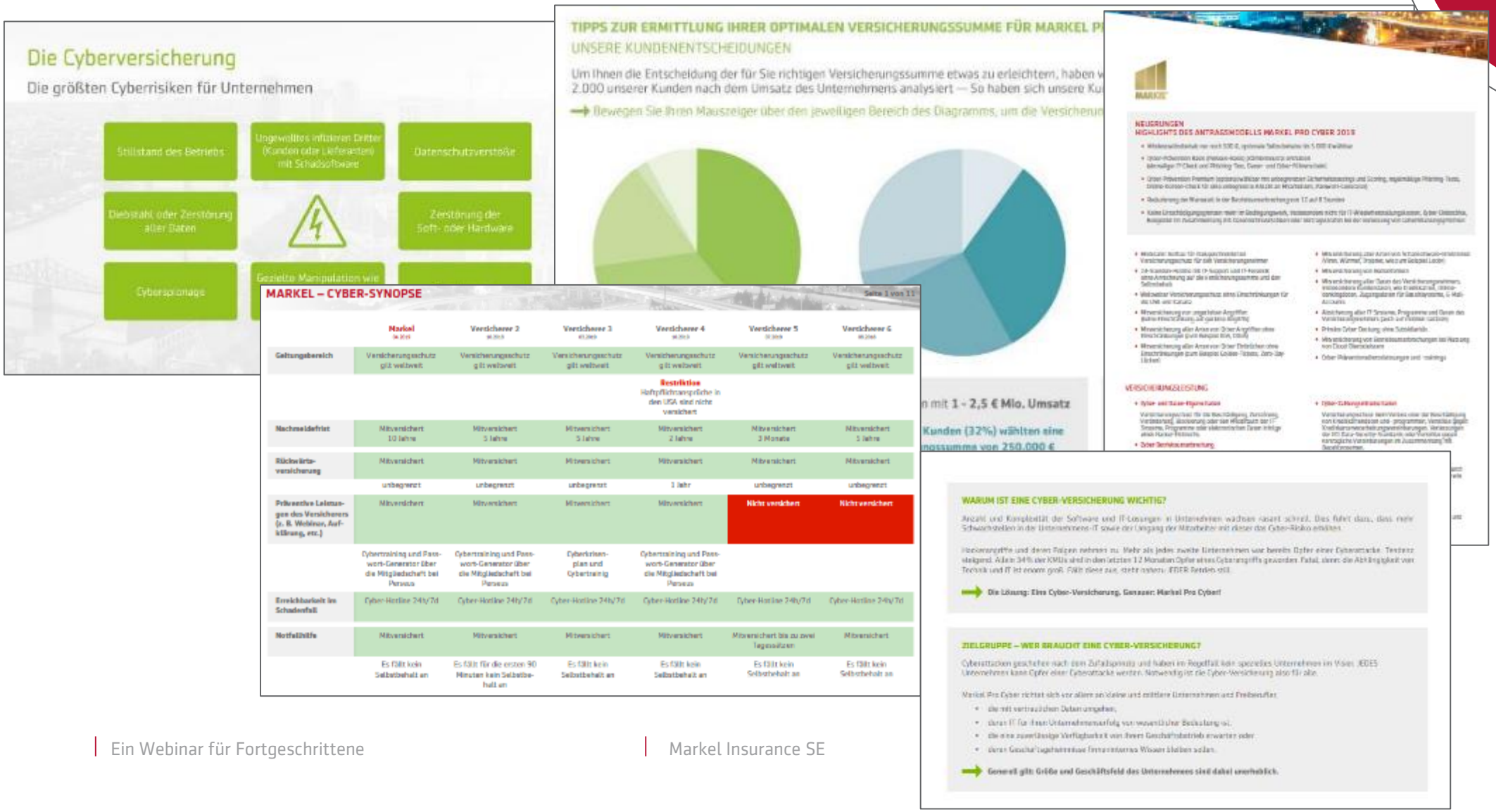
8. Der Antragsteller nutzt folgende IT-Sicherheitsvorkehrungen: JA ☐

   - Anti-Virus-Schutz mit aktuellen Virendefinitionen (Hiervon ausgenommen sind die Betriebssysteme von Apple, Unix und Linux)

Die Digitale Informationsmappe Cyber

Unterlagen für die Beratung von Cyber

5 mal Vertriebsunterstützung



Ein Webinar für Fortgeschrittene

Markel Insurance SE

07 | Über Markel

Markel

Zahlen, Daten & Fakten

Markel Insurance SE

Seit 10.2018 deutscher Versicherer

Spezialist VSH & D&O

Dynamisches Team aus 30 Mitarbeitern

Markel Corporation

Gegründet 1930 in Richmond von Sam Markel

15.600 Mitarbeiter in 21 Ländern

6,1 Mrd. USD Bruttoprämien 2017

Das Maklerportal

www.markel.de/maklerportal

Immer auf dem neusten Stand

- ✓ Keine Zugangsbeschränkung
- ✓ Immer die aktuellsten Unterlagen

Sämtliche Unterlagen & Informationen

- ✓ Alle Unterlagen zur Vertriebsunterstützung
- ✓ Antragsmodelle und Fragebögen
- ✓ Alle Ansprechpartner auf einen Blick
- ✓ Erklärfilme

Markel Academy

www.academy.markel.de

Webinare & Videos

- ✓ Kostenlos
- ✓ Einfache Bedienung
- ✓ Live und auf Band

Erklärfilme

- ✓ Kurz und einfach
- ✓ Zu verschiedenen Themen

gut beraten

- ✓ Akkreditierter Bildungsdienstleister
- ✓ Ihre Aufmerksamkeit wird belohnt!

Produktschulung

- ✓ Für Anfänger
- ✓ Und Fortgeschrittene

Markel Insurance SE

Ihr Spezialversicherer für gewerbliche Haftpflicht