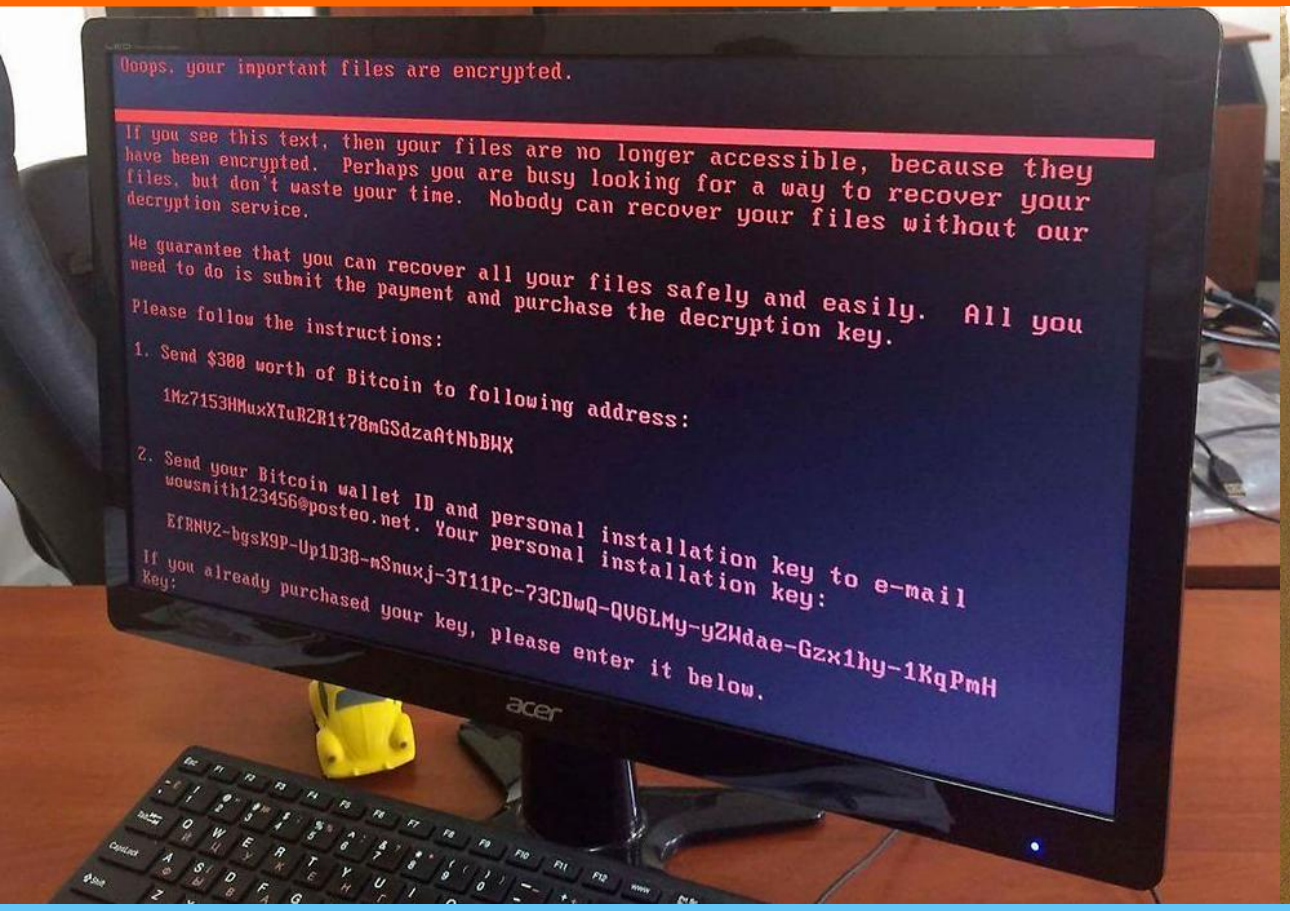
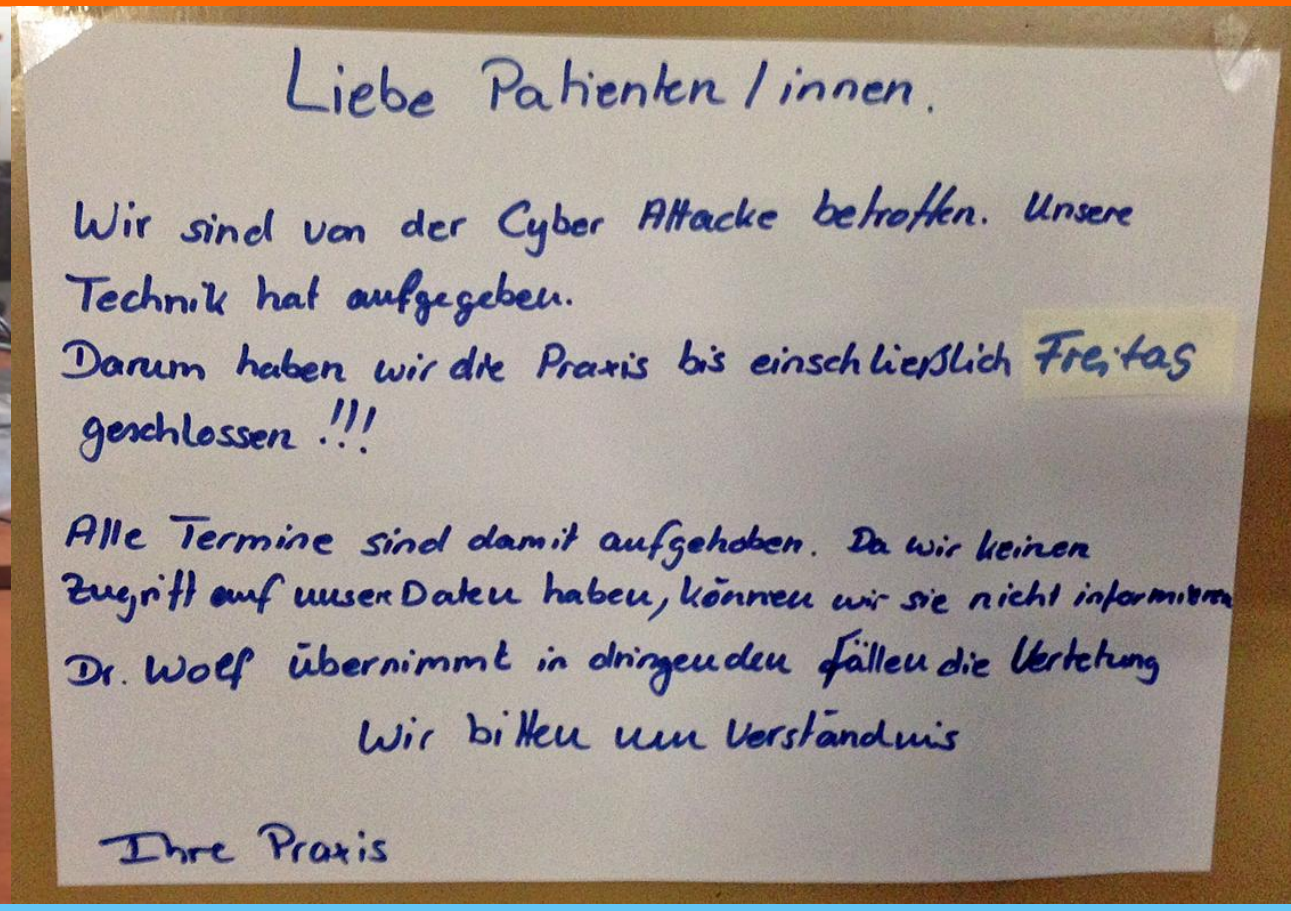
CyberDirekt

XHOCH3





Workhour – Cyber-Attacken durch Mitarbeiterprävention verhindern

CyberDirekt

XHOCH3

Anwaltskanzlei Toennes & Felsner

Gegründet 2014

35 Jahre Erfahrung in der rechtlichen Beratung kleiner & mittelständischer Unternehmen

RA Michael Kolbeck (Spezialist für IT-Recht)

Tätigkeitsschwerpunkte: Datenschutz, Computer- & Internetstrafrecht, Cyber-Crime, e-commerce,

XHoch3

Gegründet 2018

Versicherungsmakler und Unternehmensberater

35 Jahre Erfahrungen im Versicherungsgewerbe

u.a. Vorstand VGH und Alte Oldenburger Kranken

1. Cyber-Attacken und der „Risikofaktor Mensch“

2. Wie können Mitarbeiter für Cyber-Risiken sensibilisiert werden?

3. Leistungen einer Cyber-Versicherung in der Prävention sowie im Schadensfall

Agenda

Cyberkriminalität verursacht immensen Schaden

55 Mrd.€

Schäden entstanden der deutschen Wirtschaft im Jahr 2016 durch Cybercrime

80.000

polizeilich erfasste Fälle von Cyberkriminalität
im Jahr 2016

Quellen: Bitkom (2017), Manager Magazin (2017)

Der Risikofaktor Mensch einen bedeutenden Einfluss

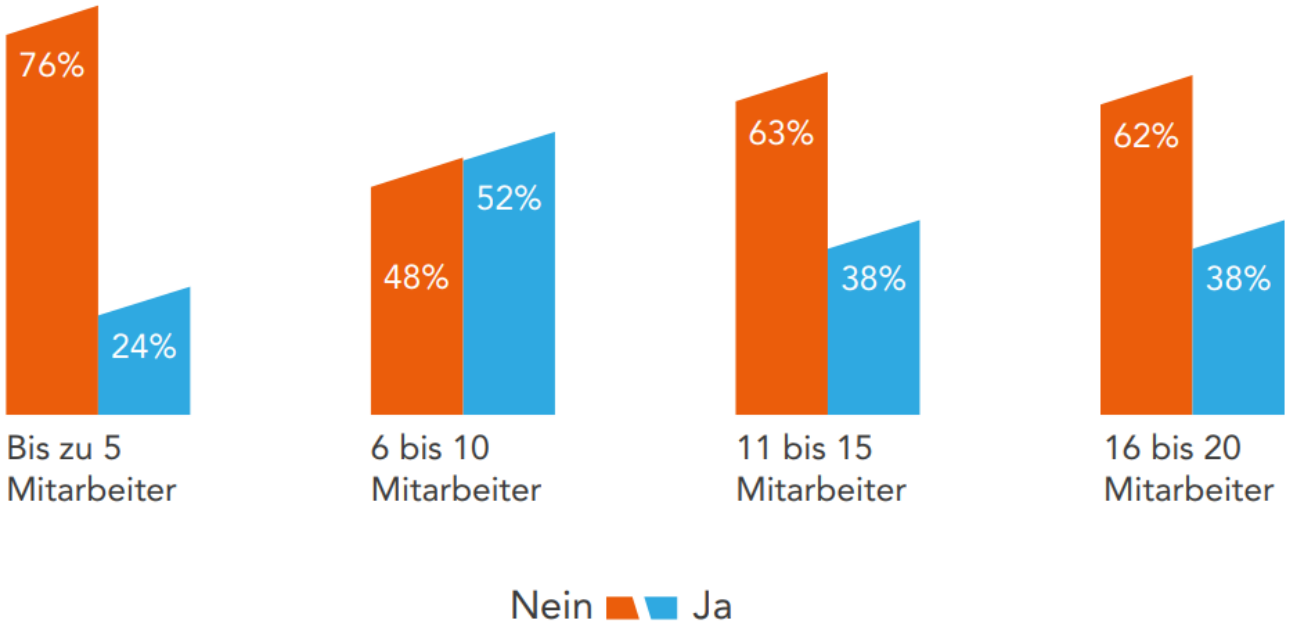
44 % der Unternehmen fühlen sich aufgrund unsachgemäßer IT-Nutzung der Mitarbeiter gefährdet

53 % der Unternehmen, die mit einem Virus angegriffen wurden, sehen uninformierte Mitarbeiter als entscheidenden Grund

Quelle: Kaspersky (2017)

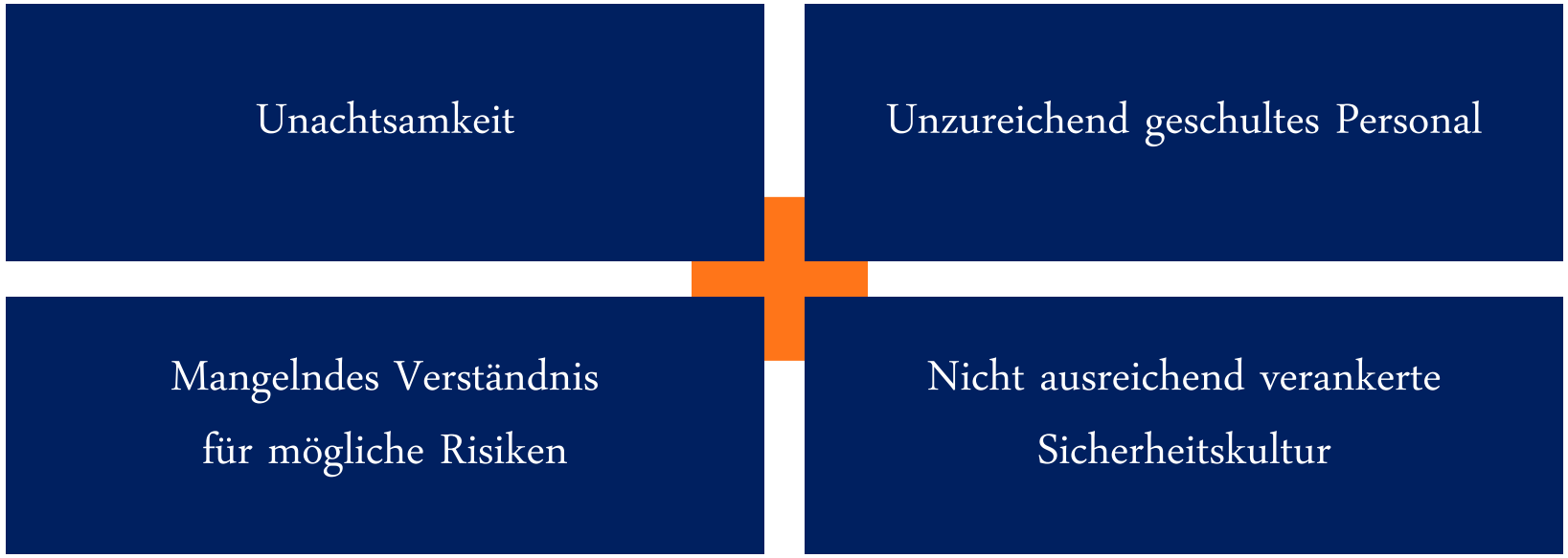
Haben Sie in den letzten 2 Jahren in Ihrem Umfeld

von einem Unternehmen gehört, das Opfer einer Cyber-Attacke geworden ist?



Cyber-Attacken und der „Risikofaktor Mensch“

Quelle: CyberDirekt / Innofact 2018


Unachtsamkeit
Unzureichend geschultes Personal
Mangelndes Verständnis für mögliche Risiken
Nicht ausreichend verankerte Sicherheitskultur

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

- Ungezielt verlaufende Cyber-Attacke, die jedes Unternehmen treffen kann
- Motiv: Erpressung von Lösegeld durch Verschlüsselung der Daten
- Risiko: Beschädigung der Daten, Betriebsunterbrechung und Datenschutzverletzung

Cyber-Attacken und der „Risikofaktor Mensch“

CyberDirekt

XHOCH3

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

1. Was ist Ransomware?
2. Woher kommt Ransomware?
3. Wie erkennt man Ransomware?
4. Wie entfernt man Ransomware?
5. Sollte ein gefordertes Lösegeld gezahlt werden?
6. Wie lässt sich vorbeugen gegen Ransomware?

Datenschutz <-> Cyber Security

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

Datenschutzverletzung?

Wenn es zu einer **Veränderung**, einem **Verlust** oder **unbefugten Zugriff** auf personenbezogene Daten gekommen ist, ist der Vorfall in jedem Fall meldepflichtig.

Sie müssen nach Paragraph 33 Abs. 1 DSGVO innerhalb von 72H die zuständige Landesdatenschutzbehörde informieren.

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

Datenschutzverletzung?

-unbewusste Veröffentlichung von personenbezogenen Daten im Internet
-Zugriff nach einer Hackerattacke auf eine Datenbank
-bloßer Verlust eines Laptops, USB-Sticks oder Mobiltelefons

Sie müssen nach Artikel 33 Abs. 1 DSGVO innerhalb von 72h die zuständige Landesdatenschutzbehörde in gesetzlich bestimmter Art & Weise (Abs. 3) informieren.

Beachte: Weitere Informationspflicht gemäß Artikel 34 DSGVO !

(https://www.lda.bayern.de/de/kleine-unternehmen.html)

CyberDirekt

XHOCH3

10. September

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

IT-SICHERHEIT

Polizei warnt: Massenhaft falsche Bewerbungen mit Viren

Ein interessantes Anschreiben ohne Rechtschreibfehler, doch im Anhang steckt ein Erpressungstrojaner. Laut Polizei hat diese Betrugsmasche gerade Konjunktur.

10. September 2018

Von Denny Gille

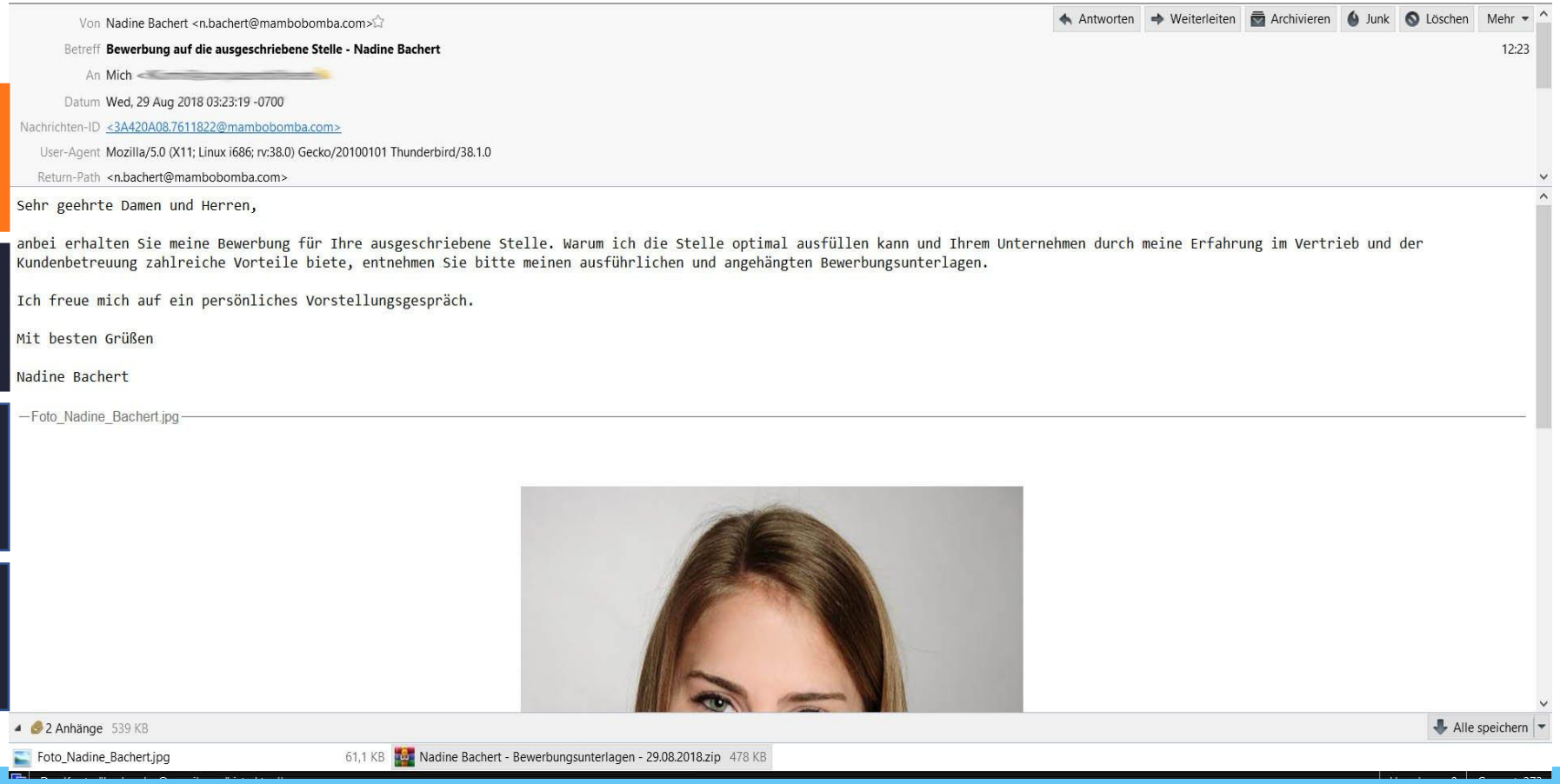
Der Mangel an Fachkräften belastet Betriebe, das neue Ausbildungsjahr beginnt – da freut man sich doch über jede Bewerbung. Oder? Diese Situation der Unternehmen nutzen Cyberkriminelle für ihre Zwecke aus. Sie versenden Bewerbungsschreiben mit Schadsoftware im Anhang. Die Masche ist nicht neu, derzeit aber seien die Schreiben „massenhaft im Umlauf", warnt die Polizei Niedersachsen.

Dabei besticht die falsche Bewerbung offenbar durch gutes Deutsch, zeigen die Beispiele, die die Polizei anführt. An der Betreffzeile „Bewerbung auf die ausgeschriebene Stelle - Nadine Bachert" ist zunächst nichts auszusetzen. Auch das E-Mail-Schreiben wirkt

CyberDirekt

XHOCH3

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter



Cyber-Attacken und der „Risikofaktor Mensch“

CyberDirekt

XHOCH3

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

Cyber-Attacken und der „Risikofaktor Mensch“

CyberDirekt

XHOCH3

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

18.9.2018 Logistikbranche - Digitale Kettenreaktion - Süddeutsche.de

Süddeutsche.de Wirtschaft

30. August 2018, 18:50 Logistikbranche

Digitale Kettenreaktion

Der Cyber-Angriff auf den Konzern Maersk zeigt die Verwundbarkeit der Transportbranche.

Von Katrin Berkenkopf

45 000 Rechner und 4000 Server musste der dänische Konzern Maersk im Sommer 2017 neu installieren. Was normalerweise ein halbes Jahr dauert, musste in zehn Tagen über die Bühne gehen. Währenddessen waren Bohrinseln in der Nordsee lahmgelegt, Container-Schiffe konnten nicht entladen werden, und Mitarbeiter an Land mühten sich mit Papier und Stift, der Flut an Arbeit Herr zu

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

INFORMATION AND COMMUNICATION TECHNOLOGY COLOGNE

IHK

ctinstanz festgelegt.

Über uns | Veröffentlichungen | IHK-Magazin | Branchen | Presse | Veranstaltungen | Kontakt | Suche ...

Home / Innovation und Umwelt / Informations- und Kommunikationstechnik / Digitalisierung allgemein

Ransomware-Attacken sind im letzten Jahr angestiegen

Es wird geschätzt, dass jeden Tag 4.000 Angriffe stattfinden.

Ransomware-Attacken sind im letzten Jahr angestiegen. Es wird geschätzt, dass jeden Tag 4.000 Ransomware-Angriffe stattfinden, ein Bericht stuft sogar Ransomware als die Nummer eins der von Cyberkriminellen im Jahr 2017 verwendeten Crimeware ein und wird als die häufigste Cyber-Erpressungsmethode identifiziert, die von Cyberkriminellen eingesetzt wird, um Unternehmen anzugreifen.

Ransomware ist eine Art von Malware, durch einen Angriff wird der Zugriff auf einen Computer oder die Daten einschränkt und dann wird Geld im Austausch für die Rückgabe der Daten verlangt. Die Schadprogramme werden dabei mittels Phishing-E-Mails, Spam-Kampagnen, Drive-Bys oder anderen Programmen verbreitet, die von einem unvorsichtigen Benutzer, auf seinen Computer heruntergeladen werden.

Die Quelle und weiteres zum Thema Schadprogramme finden Sie auf der Webseite IT-Sicherheit.

Der Objektverweis wurde nicht auf eine Objektinstanz festgelegt.

Newsletteranmeldung

Cyber-Attacken und der „Risikofaktor Mensch“

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

- Illegales Angeln von sensiblen digitalen Daten mithilfe verschiedener Köder im Internet, meist über E-Mail Anhänge
- Ziel: Erbeuten von persönlichen Daten (Kreditkartendaten, Benutzerdaten, etc.)

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

- Beispiel: Tarnung als Bank, Versicherung, Mobilfunkanbieter, Amazon, eBay, etc.
- Ziel: Erbeuten von persönlichen Daten (Kreditkartendaten, Benutzerdaten, etc.), etwa u Bankkonten zu plündern

Stadtsparkasse München

Sehr geehrter Kunde,

Da gegenwärtig die Betrügereien mit den Bankkonten von unseren Kundschaften öfters zustande kommen, sind wir genötigt, nachträglich eine zusätzliche Autorisation von den Kunden der Stadtsparkasse München durchzuführen.
Der Sicherheitsdienst von der Stadtsparkasse München hat die Entscheidung getroffen, ein neues Datensicherheitssystem einzuführen. Im Zusammenhang damit wurden von unseren Fachleuten sowohl die Protokolle der Informationsübertragung, als auch die Methode der Kodierung der übertragenen Daten neu erstellt.

Infolgedessen bitten wir Sie, eine spezielle **Form der zusätzlichen Autorisation** auszufüllen.

FORM AUSFÜLLEN

Diese Sicherheitsregeln wurden nur zum Schutz der Interessen von unseren Kunden eingesetzt.

Danke für Ihre Zusammenarbeitarbeit,
Administration der Stadtsparkasse München

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

Auf Phishing-Mail reingefallen Lazio Rom überweist Millionen-Ablöse auf falsches Konto

29.03.18, 17:33 Uhr

EMAIL FACEBOOK TWITTER MESSENGER

Claudio Lotito, Präsident von Lazio Rom, stellt im Jahr 2014 den niederländischen Innenverteidiger Stefan de Vrij als Neuzugang vor. Bei der Zahlung der Ablösesumme fielen die Italiener später aber auf einen Betrüger herein.
Foto: picture alliance / dpa

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

amazon.de

Sonntag, 12. November 2017

Von: "Amazøn.de" <info@send-mail05.trade>

Neue Meldung von Ihrem Kundenservice

Sehr geehrter Kunde,

wegen einer Gesetzesänderung sind wir verpflichtet Ihre Adressdaten sowie Ihre Zahlungsdaten zu überprüfen und eventuell zu aktualisieren

Hierzu bitten wir Sie ihre Adress- und Zahlungsdaten in einem kurzen Datenabgleich zu bestätigen.

Achten Sie auf die korrekte Eingabe Ihrer Adress- und Zahlungsdaten, sollten die von Ihnen angegebenen Daten sich zu den bereits hinterlegten Informationen unterscheiden, ist eine Legitimation nur noch postalisch möglich.

Weiter zur Verifizierung

Für mögliche Unannehmlichkeiten entschuldigt sich das Team von Amazon.de.

Mit freundlichen Grüßen
Ihr Kundenservice von Amazon.de

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

Merkmale einer Phishing-Mail/ -Website

- Mailheader
- Mails in fremder Sprache
- Fehlender Name
- Dringender Handlungsbedarf/ Androhung von Konsequenzen
- Eingabe von Daten
- Aufforderung zur Öffnung von Anhängen/ Links/ Dateien
- Links oder eingefügte Formulare
- Bisher noch nie E-Mails von der Bank erhalten oder kein Kunde
- Grammatik- und Orthografie-Fehler

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

Merkmale einer Phishing-Mail/ -Website

- Fehlen des Kürzels "https://"
- Adresszeilen sehen den echten nur ähnlich, enthalten jedoch unübliche Absätze, Zahlen, verdrehte Buchstaben…
- PIN-/ TAN-Codes werden oft abgefragt
- nur wenige weitere Funktionen/ nicht klickbare „Links“

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

- Täter nutzen menschliche Eigenschaften und Verhaltensweisen als Angriffsfläche

stern

NEON NIDO VIEW STERN TV

VIDEO SPIELE ABO FOTOGRAFIE

Panorama Politik Kultur Lifestyle Digital Wirtschaft Sport Gesundheit Genuss Reise Familie Auto

Home > Wirtschaft > News > Bäckerei-Angestellte überweist 1,9 Millionen an Trickbetrüger

Auf Chef-Trick reingefallen

15. Juli 2017 14:31 Uhr

Bäckerei-Angestellte überweist 1,9 Millionen Euro an Trickbetrüger

Sie dachte, die Anweisung käme von der Chefin, stattdessen überwies die Buchhalterin einer Münchner Bäckereikette 1,9 Millionen Euro an Trickbetrüger aus Hongkong. Nun wird vor Gericht gestritten, wer den Schaden bezahlen muss.

Drucken

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

- Fake President: Täter geben sich gegenüber Mitarbeiter der Buchhaltung als Geschäftsführer aus, um diesen zu einer Überweisung von Geldbeträgen zu bewegen
- USB-Sticks ausgelegt auf Firmenparkplatz. Neugierde der Mitarbeiter führt zur Nutzung auf Firmenrechner.

stern

NEON NIDO VIEW STERN TV

VIDEO SPIELE ABO FOTOGRAFIE

Panorama Politik Kultur Lifestyle Digital Wirtschaft Sport Gesundheit Genuss Reise Familie Auto

Auf Chef-Trick reingefallen

15. Juli 2017 14:31 Uhr

Bäckerei-Angestellte überweist 1,9 Millionen Euro an Trickbetrüger

Sie dachte, die Anweisung käme von der Chefin, stattdessen überwies die Buchhalterin einer Münchner Bäckereikette 1,9 Millionen Euro an Trickbetrüger aus Hongkong. Nun wird vor Gericht gestritten, wer den Schaden bezahlen muss.

Drucken

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

NEUE OZ OSNABRÜCKER ZEITUNG

... schreibt am 13.07.2016:

- **Betrugsversuch im Landkreis Osnabrück: Mit neuem Cheftrick beinahe eine Million abkassiert**
- Die Täter geben sich als Chef eines Unternehmens aus und drängen den Buchhalter zur Eile. Für die Übernahme von ausländischen Firmenanteilen müsse schnell viel Geld überwiesen werden.
- Eine Firma aus dem Landkreis Osnabrück ist beinahe auf den neuen Cheftrick hereingefallen. Ein Schaden von knapp 1 Mio. Euro konnte gerade noch abgewendet werden. Die an den Enkeltrick angelehnte Masche ist im Osnabrücker Land angewendet worden.

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

NEUER CFO RÄUMT AUF

12.04.17 08:10

Leoni arbeitet Fake-President-Fall auf

40 Mio € Verlust

Von Jakob Eich

Kriminelle klauten dem Autozulieferer Leoni mit dem Chef-Betrug im vergangenen Sommer 40 Millionen Euro. Die Franken arbeiten den Fall auf – und ziehen personelle Konsequenzen.

+ meine Artikel

CyberDirekt

XHOCH3

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

AUTOR

JOCHEN SAAL

Rechtsanwalt
Fachanwalt für Arbeitsrecht
Partner

Rechtsanwalt Jochen Saal, Partner, gehört seit November 2007 zum Arbeitsrechtsteam von KLIEMT.Arbeitsrecht in Düsseldorf. Der Schwerpunkt seiner Tätigkeit liegt in der gerichtlichen und außergerichtlichen Beratung von Unternehmen und Führungskräften in sämtlichen Fragen des Arbeitsrechts. Besondere Expertise besitzt Rechtsanwalt Saal zudem im Bereich der betrieblichen Altersversorgung.

Kontaktdaten
vCard downloaden
Alle Beiträge lesen

NÄCHSTES THEMA

Neues vom BAG: Ob Feier oder Nacht, alles wird mit Mindestlohn gemacht?

ARBEITSRECHT IN DEUTSCHLAND / COMPLIANCE 0

Update zur „Chef-Masche“: Sächsisches LAG verurteilt Arbeitnehmerin zum Schadensersatz in Höhe von 150.000 €!

VON JOCHEN SAAL - 26. SEPTEMBER 2017

Cyber-Attacken und der „Risikofaktor Mensch“

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

- Bei unbekannten oder auffällig stark nachfragenden Absendern, Anrufern, Besuchern zunächst deren Identität verifizieren (möglichst über offizielle/ öffentliche Wege kontaktieren und nicht über Kontaktinformationen, die auf einer mit der Anfrage verbundenen Website bereitgestellt werden)
- Bei Beantwortung, möglichst wenige persönl./ geschäftl./ finanzielle Infos preisgeben
- Keine Links aus E-Mails verwenden, welche die Eingabe persönlicher Daten verlangen; stattdessen URL selbst im Browser eingeben

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

- Achtsamkeit erst recht bei angeblicher Dringlichkeit/ angedrohten Konsequenzen
- Beachtung der angegebenen URLs/ Vergleich mit offiziellen URLs (.ru?)
- Technische & Organisatorische Maßnahmen: 1. Antivirensoftware, Firewalls, E-Mail-Filter & alle Anti-Phishing-Funktionen des Email-Clients & Webbrowsers installieren, nutzen & pflegen;

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

Der Angriff kann auch von innen kommen

Mit Cyberattacken lassen sich Betriebe lahmlegen. Diese Gefahr kommt in den Unternehmen an. Versicherer wittern ihre Chance.

pik. FRANKFURT, 30. Juli. Solche Fälle kann man sich nicht ausdenken, die kann nur das Leben schreiben: Ein Mitarbeiter aus der Informationstechnik überwirft sich mit seinem Unternehmen und verliert seine Stelle. Dabei wird allerlei schmutzige Wäsche gewaschen, so dass er wilde Rachegelüste entwickelt. Er legt sich einen Schlachtplan zurecht, den er akribisch in einem Aktenordner dokumentiert, und dringt mit seinem Insiderwissen in das Firmennetzwerk ein. Über das Darknet führt er seinen Rachekrieg. Auf einmal kommen Internetuser nicht mehr auf die Seite von Kommunen, für die das Unternehmen als Dienstleister tätig ist, sondern auf Pornoseiten. Jeden Tag entsteht mehr Chaos, die Unternehmensführung ist verzweifelt.

Der Fall hat im vergangenen Jahr den größten Cyberschaden eines Versicherers in Deutschland ausgelöst. 3 Millionen Euro betrugen die Kosten für IT-Forensik, Krisenkommunikation und für Betriebsun-

3 Mio. € Schaden

Cyber-Attacken und der „Risikofaktor Mensch“

1. Ransomware
2. Phishing
3. Social Engineering
4. Innentäter

DIE HAFTUNG

Vorsatz <-> Fahrlässigkeit

- Datenschutzbeauftragter?
- Leiter der IT-Abteilung?
- Mitarbeiter (z.B. Personaler oder Buchhalter)?
- Externer IT-Dienstleister/ Fernbetreuer/ Hoster?
- Geschäftsführer?
- § 130 OWiG: „Inhaber eines Betriebs oder Unternehmens“ = Geschäftsführer
- Art. 5 f), 32 DSGVO: 1. „Verantwortlicher“ (i.d.R. Geschäftsführer) & 2. „Auftragsverarbeiter“ (z.B. ext. IT-Dienstleister)
- § 43 GmbHG: „Geschäftsführer“ = Geschäftsführer!

1. Cyber-Attacken und der „Risikofaktor Mensch“

2. Wie können Mitarbeiter für Cyber-Risiken sensibilisiert werden?

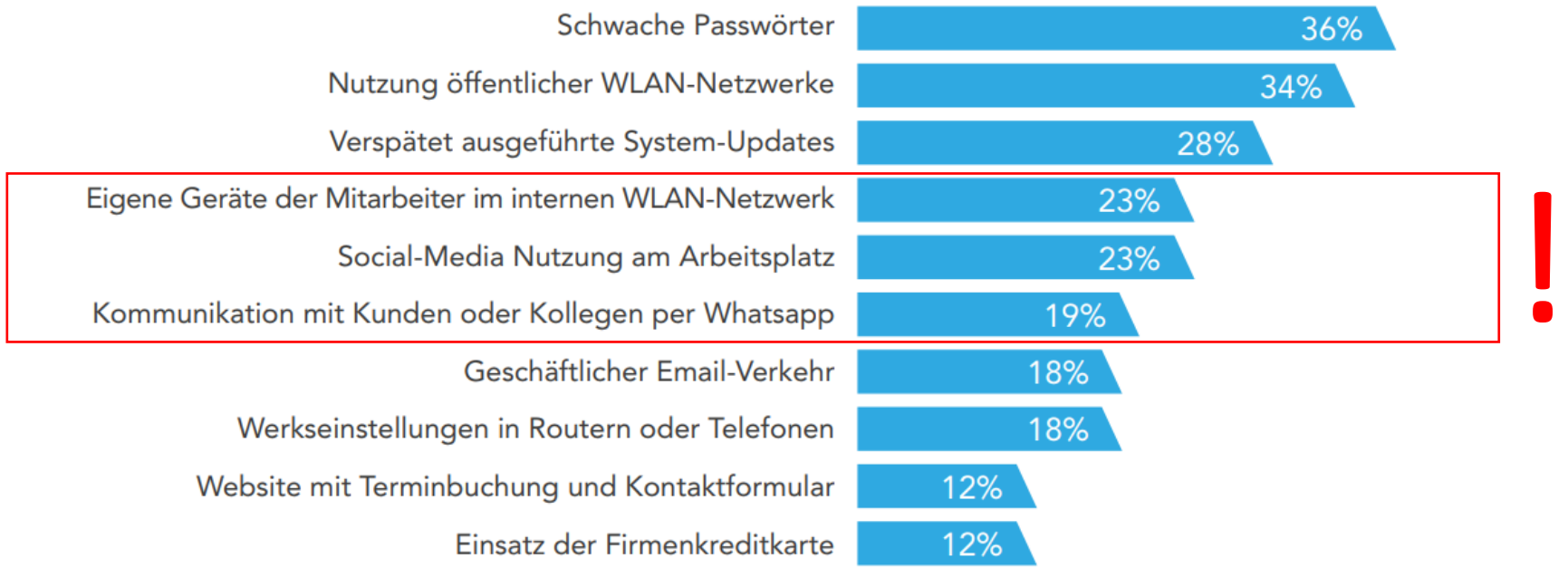
3. Leistungen einer Cyber-Versicherung in der Prävention sowie im Schadensfall

Agenda

Was ist Ihrer Meinung nach die größte Gefahrenquelle von Cyber-Attacken in Ihrem Arbeitsumfeld?

Wie können Mitarbeiter für Cyber-Risiken sensibilisiert werden?

Quelle: CyberDirekt / Innofact 2018



Wie können Mitarbeiter für Cyber-Risiken sensibilisiert werden?

Quelle: CyberDirekt / Innofact 2018

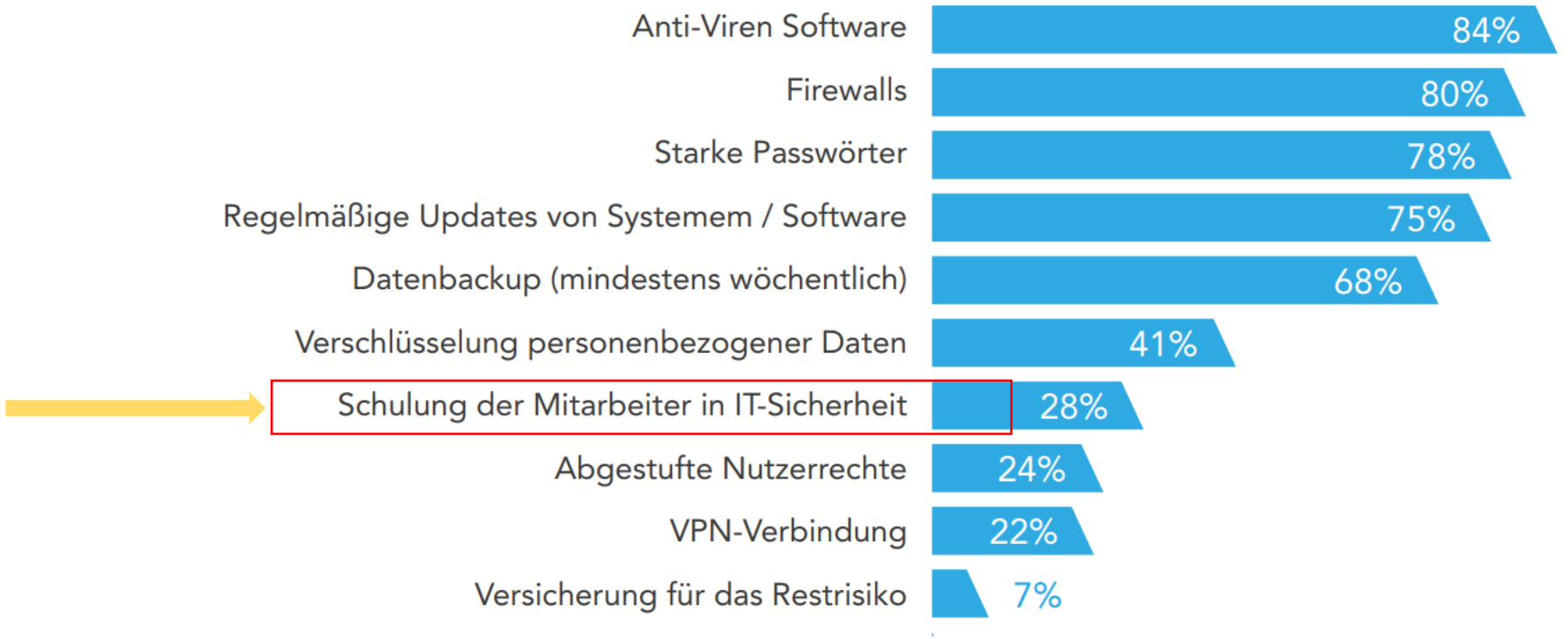
CyberDirekt

XHOCH3

Welche Maßnahmen zur Absicherung gegen die Folgen von Cybercrime (Hackerangriffe, Datendiebstahl etc.) nutzen Sie in Ihrem Unternehmen?

Wie können Mitarbeiter für Cyber-Risiken sensibilisiert werden?

Quelle: CyberDirekt / Innofact 2018



Wie können Mitarbeiter für Cyber-Risiken sensibilisiert werden?

Quelle: CyberDirekt / Innofact 2018

Entlastungsnachweis/ Nachweis CS-Niveau

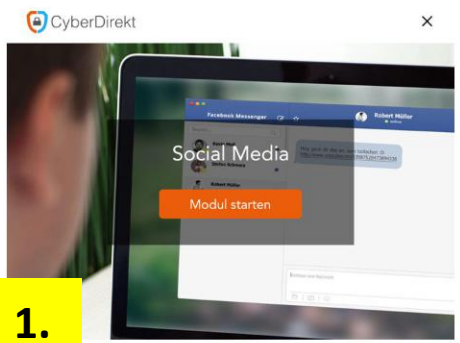
- Belehrung über Verpflichtung/ Vereinbarung zur Wahrung von **Geschäfts- & Betriebsgeheimnissen**
- Unterrichtung & Vertraulichkeitsverpflichtung der Mitarbeiter auf das **Datengeheimnis**
- Konzernrichtlinie/ Gesellschafterbeschluss zur Einführung einer Datenschutz-Organisation
- Unternehmensrichtlinien zum Datenschutz/ IT-**Sicherheitskonzept** für Mitarbeiter
- Richtlinien zur Nutzung von **Internet & Email** am Arbeitsplatz/ Home-Office bzw. Mobile-Office (Telearbeit)
- **Dokumentation**!!!

Wie können Mitarbeiter für Cyber-Risiken sensibilisiert werden?

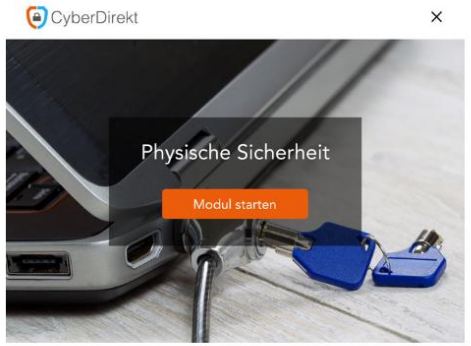
Quelle: CyberDirekt / Innofact 2018

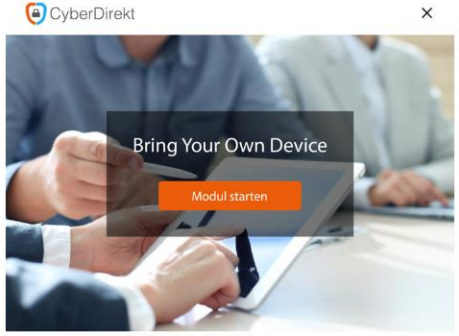
CyberDirekt

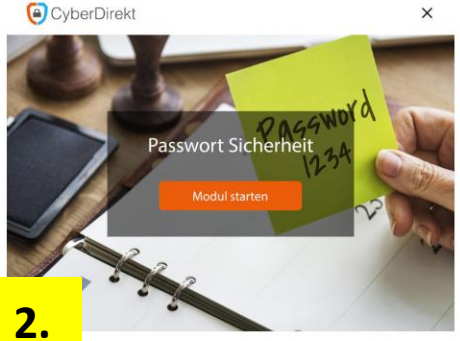
XHOCH3



1.



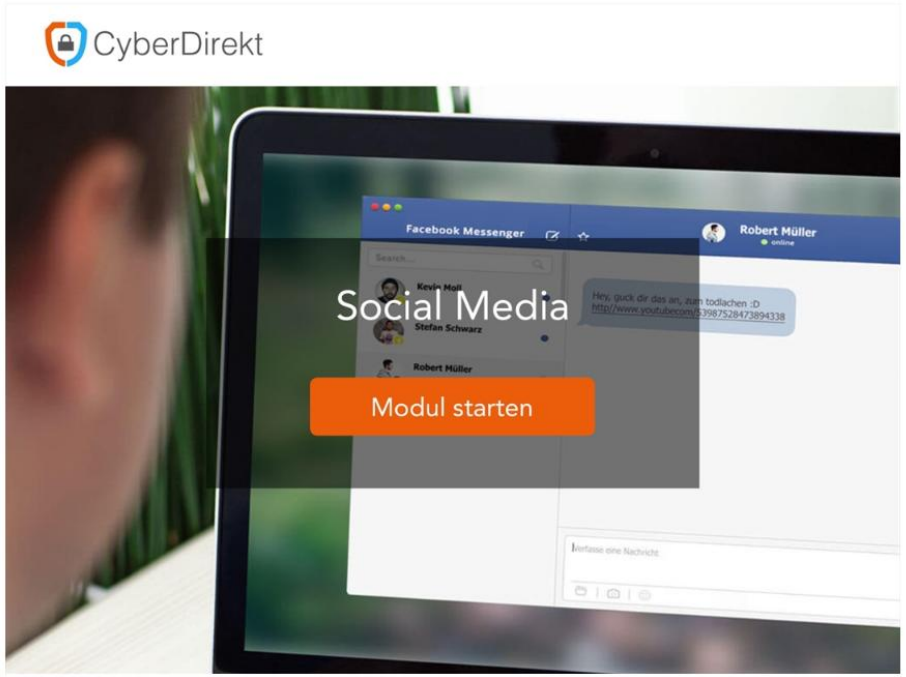




2.

Wie können Mitarbeiter für Cyber-Risiken sensibilisiert werden?

CyberDirekt



Wie können Mitarbeiter für Cyber-Risiken sensibilisiert werden?

CyberDirekt

CyberDirekt

Einführung | Modul | Quiz

Wie kann ich Cyber Angriffe über soziale Medien erkennen?

„Zu gut, um wahr zu sein" -
Ihnen werden unrealistische Versprechungen gemacht

- **Geld**: Es wird Ihnen versprochen, in **kurzer Zeit** mit einfachen Mitteln **sehr viel Geld zu verdienen**
- **Rabattpreise**: Sie erhalten **unrealistische Rabatte** für meist **hochwertige Produkte**

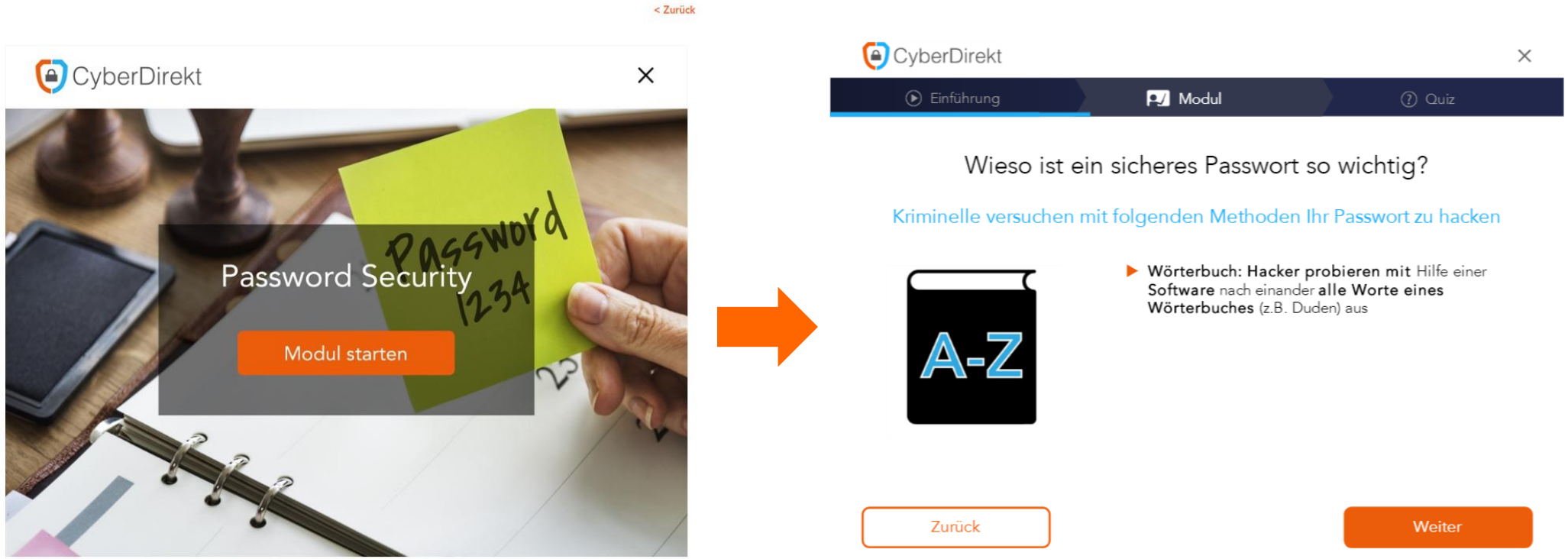
Zurück | Weiter

ACHTUNG!

Wie können Mitarbeiter für Cyber-Risiken sensibilisiert werden?

CyberDirekt

XHOCH3



Wie können Mitarbeiter für Cyber-Risiken sensibilisiert werden?

Pingsmann221080!

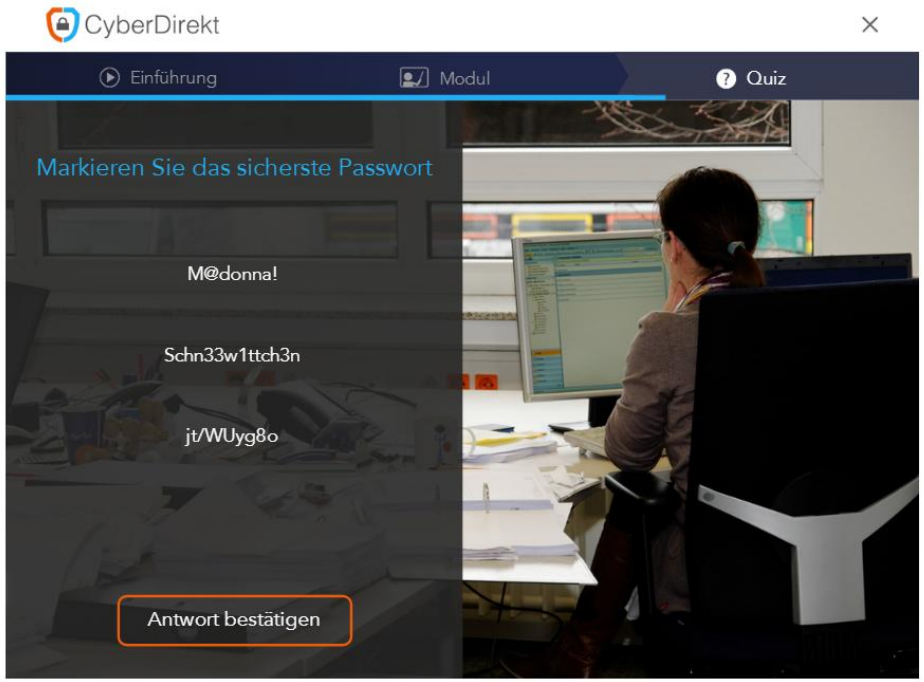
Sommerurlaub2012#Borkum

NinaTobiasMaximilian

Nicht sicher!

Wie können Mitarbeiter für Cyber-Risiken sensibilisiert werden?

CyberDirekt



Wie können Mitarbeiter für Cyber-Risiken sensibilisiert werden?

CyberDirekt

XHOCH3

1. Cyber-Attacken und der „Risikofaktor Mensch“

2. Wie können Mitarbeiter für Cyber-Risiken sensibilisiert werden?

3. Leistungen einer Cyber-Versicherung in der Prävention sowie im Schadensfall

Agenda

CyberDirekt

XHOCH3

Was leistet eine Cyber-Versicherung?

„Vollkasko-Versicherung für Ihre IT-Systeme“

Übernahme aller Kosten, die durch einen Hacker-Angriff auf die IT-Systeme Ihrer Firma entstehen können. Erstattung von Umsatzausfall sowie sofortige 24/7 Hilfe im Schadenfall durch Spezialisten.

Was leistet eine Cyber-Versicherung?

„Haftpflichtversicherung für Ihre IT-Systeme“

Abwehr von Schadensersatzansprüchen aufgrund von Datenschutzverletzungen.

Abwehrkosten bei behördlichen Ordnungswidrigkeiten- und Strafverfahren versichert, so lange kein Vorsatz vorliegt.

CyberDirekt

XHOCH3

1. Eigenschäden
2. Assistance-Leistungen
3. Drittschäden
4. Sonstige Regelungen

- Identifikation und Beweissicherung des Vorfalls (IT-Forensik)
- Wiederherstellungskosten für Daten und Systeme
- Betriebsunterbrechung
- Abwehr einer Cyber-Bedrohungslage / Erpressung
- Beratung zu gesetzlichen Pflichten des Datenschutzes und Kosten für die Benachrichtigung Betroffener

Überblick Cyber-Versicherungen allgemein

CyberDirekt

XHOCH3

1. Eigenschäden
2. Assistance-Leistungen
3. Drittschäden
4. Sonstige Regelungen

- 24/7 Hotline für Soforthilfe im Notfall
- Telefonische Erstberatung bei begründetem Verdacht
- Kosten für Krisen- / PR Beratung und PR-Maßnahmen
- Kosten für Einsatz eines Call-Centers

CyberDirekt

HOCH 3

1. Eigenschäden
2. Assistance-Leistungen
3. Drittschäden
4. Sonstige Regelungen

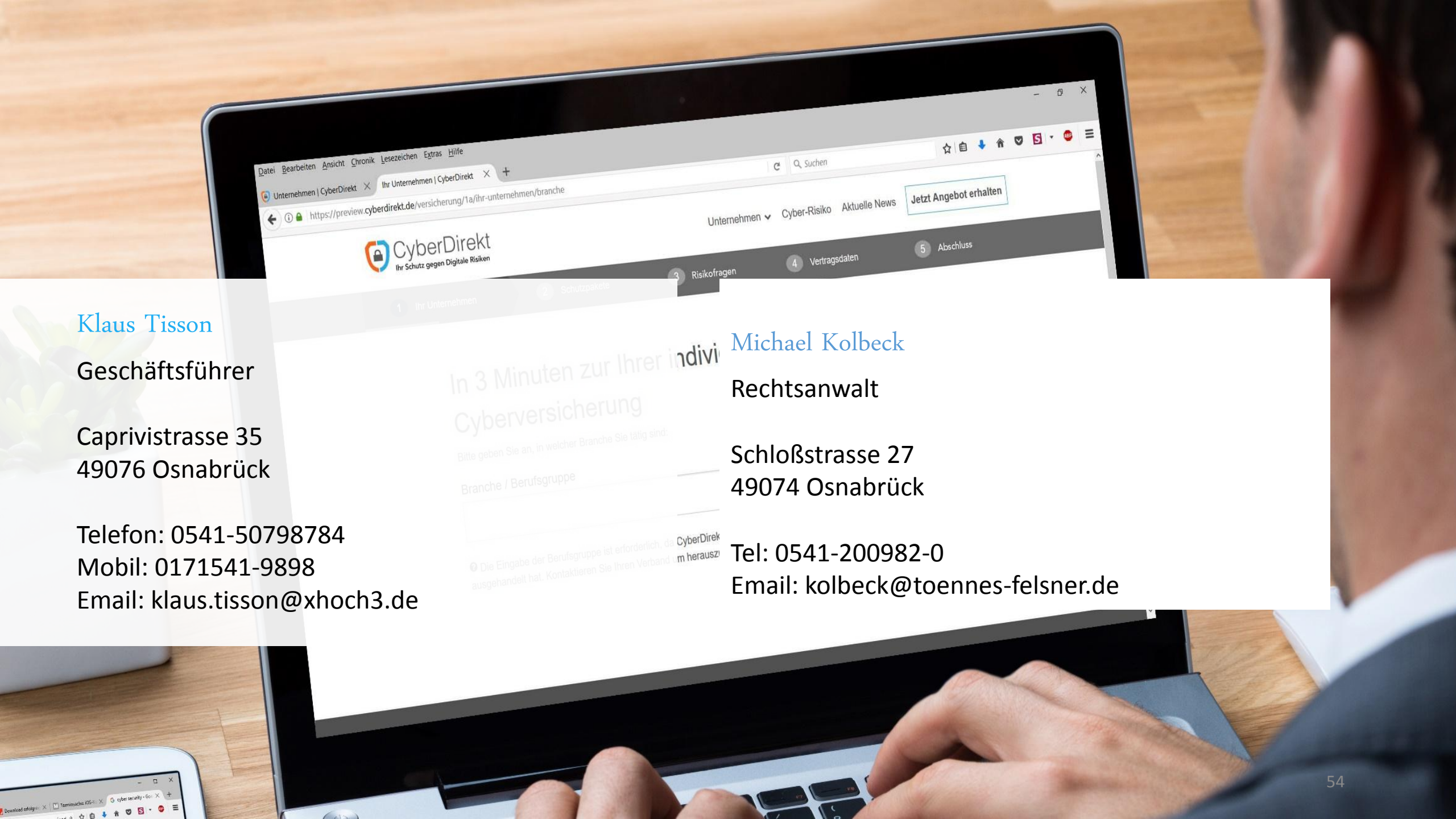
- Persönlichkeitsrechts-Verletzung
- Abwehr unberechtigter Schadensersatzansprüche
- Abwehrkosten bei behördlichen Ordnungswidrigkeiten- und Strafverfahren versichert, so lange kein Vorsatz vorliegt
- Daten- und Vertraulichkeits-Verletzung
  - Unbeabsichtigte oder fahrlässige Veröffentlichung von Daten
  - Unberechtigter Zugriff oder unberechtigte Nutzung von Kundendaten aus dem IT-Systems des VN

CyberDirekt

XHOCH3

1. Eigenschäden
2. Assistance-Leistungen
3. Drittschäden
4. Sonstige Regelungen

- Beitragsfreie, unbegrenzte Rückwärtsdeckung
- Vermögensschaden inkl. Datenschäden
- Versicherungssumme steht 1x pro Jahr zur Verfügung
- Laufzeit 1 Jahr mit automatischer Verlängerung
- Beantwortung der Risikofragen durch VN



Klaus Tisson

Geschäftsführer

Caprivistrasse 35
49076 Osnabrück

Telefon: 0541-50798784
Mobil: 0171541-9898
Email: klaus.tisson@xhoch3.de

Michael Kolbeck

Rechtsanwalt

Schloßstrasse 27
49074 Osnabrück

Tel: 0541-200982-0
Email: kolbeck@toennes-felsner.de