Ihre Referenten:

Ingo Steinwedel

Produktförderer MultiLine

Firmenkunden Business Consulting

Telefon: 0611 533-73945

Mobil: 0151 26413834

E-Mail: Ingo.Steinwedel@ruv.de

Dominik A. Baumann, Ass Jur.

Key Account Manager

Abteilung Banken/VSV

Telefon: 0611 533-2452

Mobil: 0151 26417983

E-Mail: Dominik.Baumann@ruv.de

Sinsheim, 17.10.2023

Dominik Baumann, Key Account Manager Banken/ Kredit
Ingo Steinwedel, Firmenkunden Business Consulting

Cybercrime – Die unterschätzte Gefahr

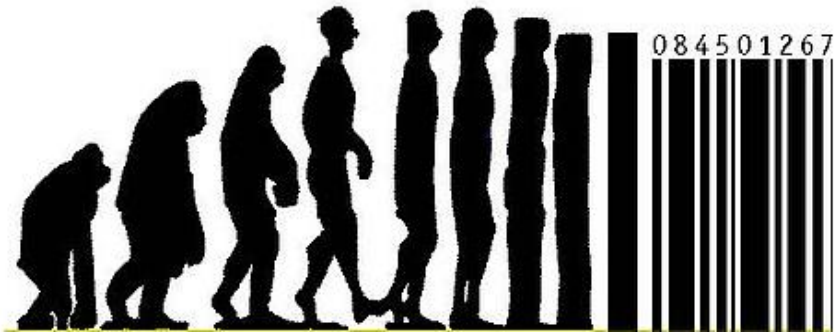
Du bist nicht allein.

Hinterlistige Attacke in Ostfriesland

Die unterschätzte Gefahr

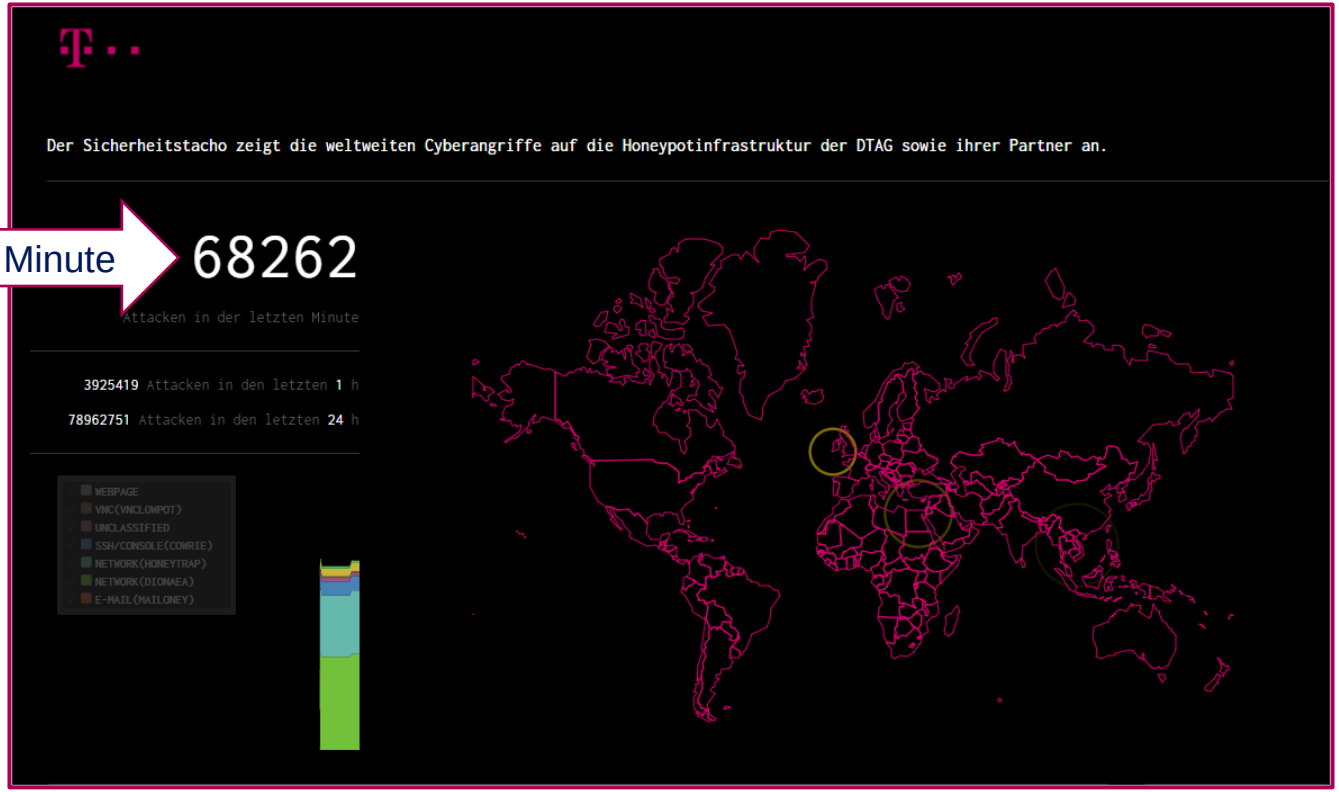
Die aktuelle Bedrohungslage Cyberkriminalität

- Der weltweite Schaden durch Sturm und Naturkatastrophen beträgt 200 Mrd. €
- Der weltweite Schaden durch Cyberkriminalität beträgt 600 Mrd. €
- Ungefähr 6.172 mittelständische Unternehmen werden pro Tag gehackt
- Die Gefahr gehackt zu werden ist 30 mal höher, als von einem Feuerschaden betroffen zu sein
- Der durchschnittliche Schaden beläuft sich auf
  - 193.000,- € bei kleinen und mittelständischen Unternehmen
  - 511.400,- € in der Baubranche



Die unterschätzte Gefahr

Wer soll uns denn schon hacken?



Angriffe pro Minute

CyberRisk - Zahlen, Daten, Fakten

Kennzahlen zum Thema Cyber-Kriminalität:

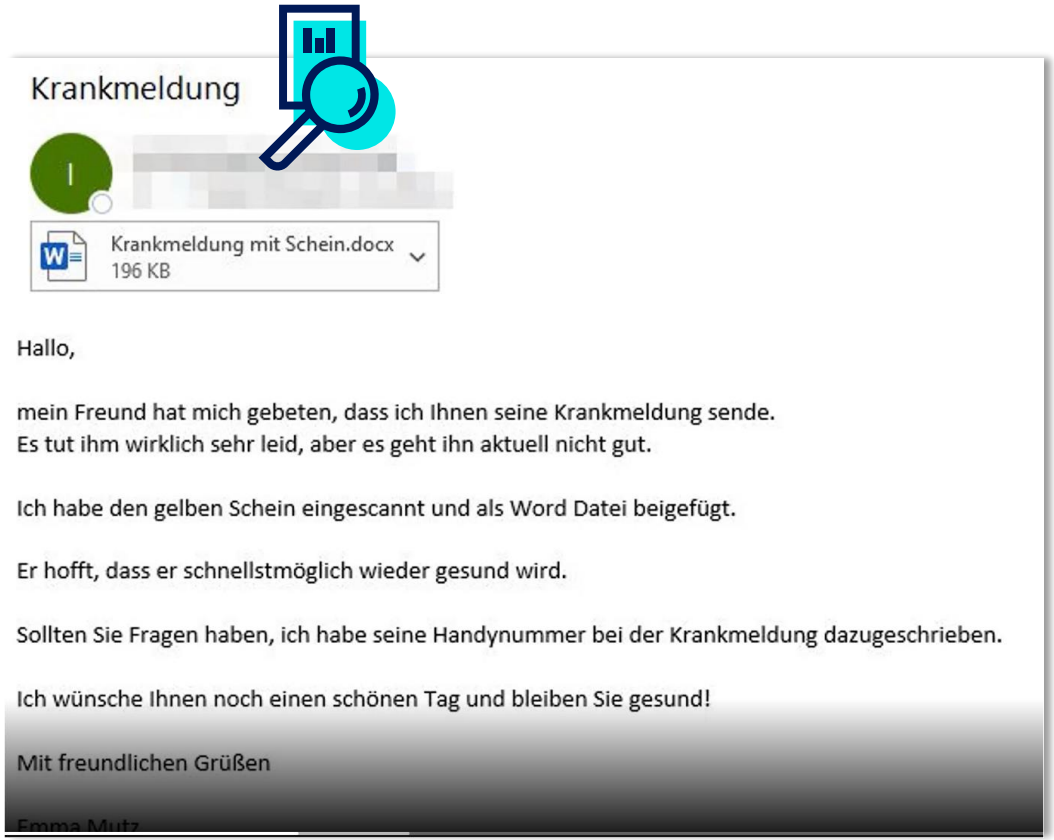
- 206 Milliarden Euro Schaden jährlich bei deutschen Unternehmen
- Allein 41,5 Milliarden Euro Schaden jährlich allein durch Ausfall Produktionssysteme oder Betriebsabläufe
- 300 Millionen Schadprogramme weltweit
- täglich 300.000 neue Varianten von Schadprogrammen
- Ca. 60 global agierende Cybercrime-Organisationen
- BSI meldet jährlich rund 15 Mio. Schadprogramm-Infektionen an deutsche Netzbetreiber
- Fast jedes zweite Unternehmen wurde in den letzten 12 Monaten Opfer eines Angriffs (84%)
- Durchschnittliche Höhe Cyber-Schäden bei kleinen und mittelständischen Unternehmen steigt rasant
- In 51% der Schadenfälle bei kleinen und mittelständischen Unternehmen dauert die Betriebsstörung deutlich länger als 1 Tag, teilweise Monate

Was ist das Cyber-Risiko?

- Warum ist praktisch jedes Unternehmen von der Bedrohungslage betroffen?

  - Eine 100-prozentige Sicherheit beim dienstlichen Umgang mit elektronischen Daten kann trotz aller vorbeugender Schutzmaßnahmen auch die beste IT-Abteilung nicht gewährleisten!
  - Es verbleibt immer ein „Risikosumpf“, der immer größer wird.
  - Es gibt nur noch 2 Arten von Unternehmen: Die, die bereits gehackt wurden und die, die noch gehackt werden
  - Cyber-Kriminalität als „Geschäftsmodell“: Cyber-Crime ist inzwischen lukrativer als Drogenhandel
    - besonders beliebt: Erpressung
    - besonders beliebt: Verkauf der erbeuteten Daten im Darknet
    - besonders beliebt: „Social Engineering“
    - neuer Wirtschaftszweig: „Crime as a service“, „RaaS“ (= Ransom as a Service)

Der Mensch wird „gehackt“



Gründe,
warum Mitarbeiter kriminell werden:

- Persönlicher oder finanzieller Profit
- Aufwändiger Lebensstandard, Sucht
- Engagement, Geltungsbedürfnis
- Niedrige Hemmschwelle und Mangel an Unrechtsbewusstsein
- Ehrgeiz, Verbesserung der sozialen Stellung, Habgier
- Frustration und Wut über Arbeitgeber
- Günstige Gelegenheit durch unzureichende interne Kontrollen
- Beeinflussung durch anderweitige Abhängigkeit
- Inflation und wirtschaftlicher Abschwung!

[Vertrauensschadenversicherung wird wichtiger - Versicherungsmagazin.de]

NW+ Warburg/Paderborn

Mitarbeiter soll fast 900.000 Euro veruntreut haben

Der 55-jährige Ex-Angestellten einer Warburger Firma muss sich vor dem Paderborner Landgericht verantworten. Ihm droht eine lange Haftstrafe.

6000 Liter Bier unterschlagen

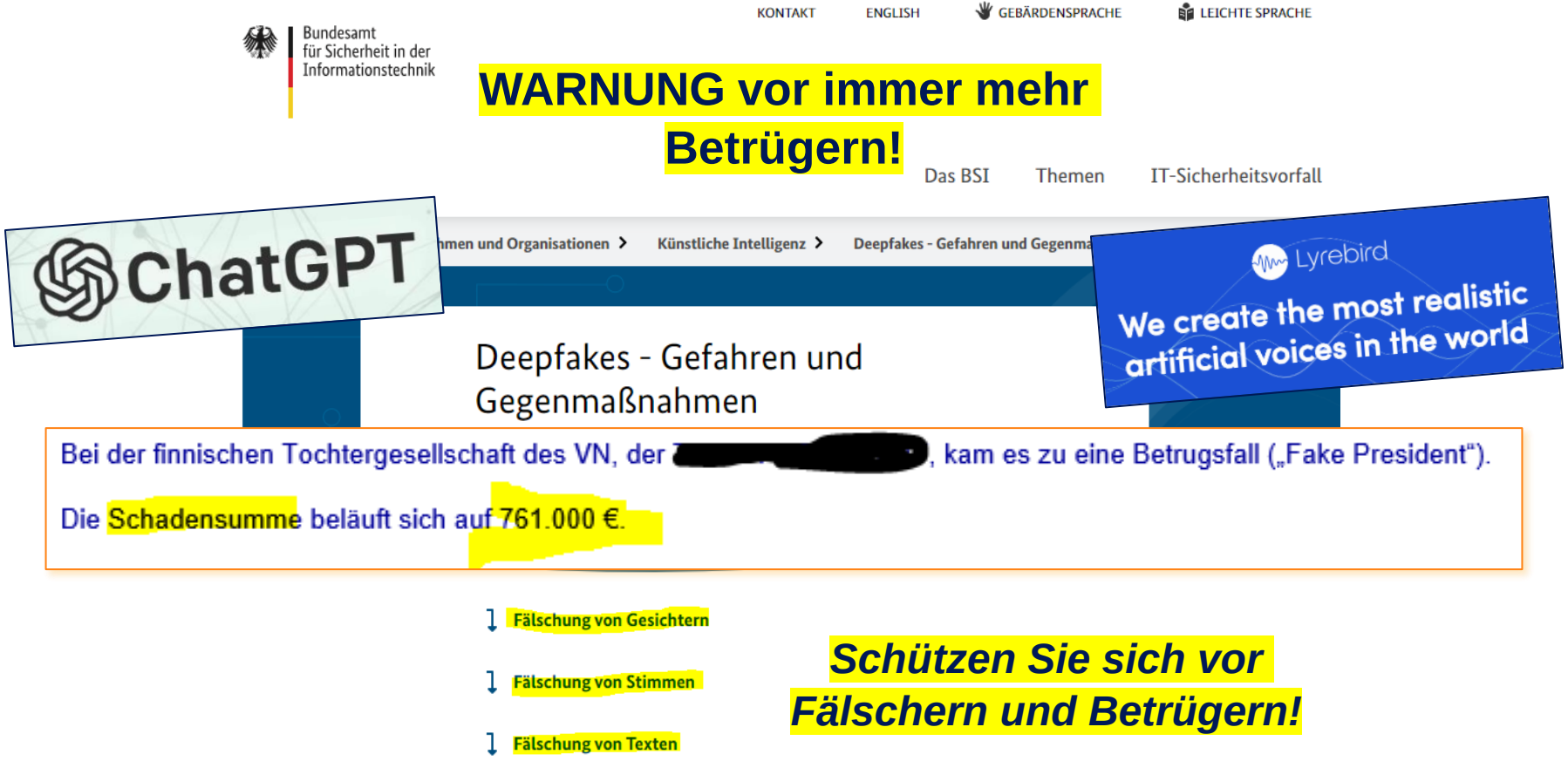
PROZESS Geldstrafe für städtischen Mitarbeiter

FRANKFURT (dpa). Weil er als [illegible] der Protokollabteilung der Stadt Frankfurt insgesamt 6000 Liter Fassbier unterschlagen und auf eigene Rechnung verkauft hatte, ist ein 51 Jahre alter Mann am Dienstag in Frankfurt zu 1600 Euro Geldstrafe (200 Tagessätze) verurteilt worden. Das Amtsgericht erließ einen entsprechenden Strafbefehl, nachdem der Angeklagte nicht vor Gericht erschienen war und nur seine Verteidigerin geschickt hatte.

Die Anklage ging davon aus, dass er in mehreren Tranchen bis 2011 bei einer Frankfurter Getränkehandlung immer wieder Fassbier für städtische Empfänge bestellte, obwohl das Bier infolge von Sponsoren gar nicht hätte gekauft werden müssen. Das Bier wurde von dem Angeklagten an Wirte in der Frankfurter Innenstadt oder über den eigenen Partyservice verkauft. Die Staatsanwaltschaft geht bei insgesamt 138 Fass zu je 30 oder 50 Liter von einem Schaden von rund 18 000 Euro für die Kommune aus.

Nach dem Bekanntwerden der Vorwürfe hatte sich die Stadt von dem Mitarbeiter getrennt. Ihm bleibt nach Angaben des Gerichts nun die Möglichkeit, den Strafbefehl zu akzeptieren oder aber Einspruch einzulegen. Dann würde erneut eine Verhandlung anberaumt.

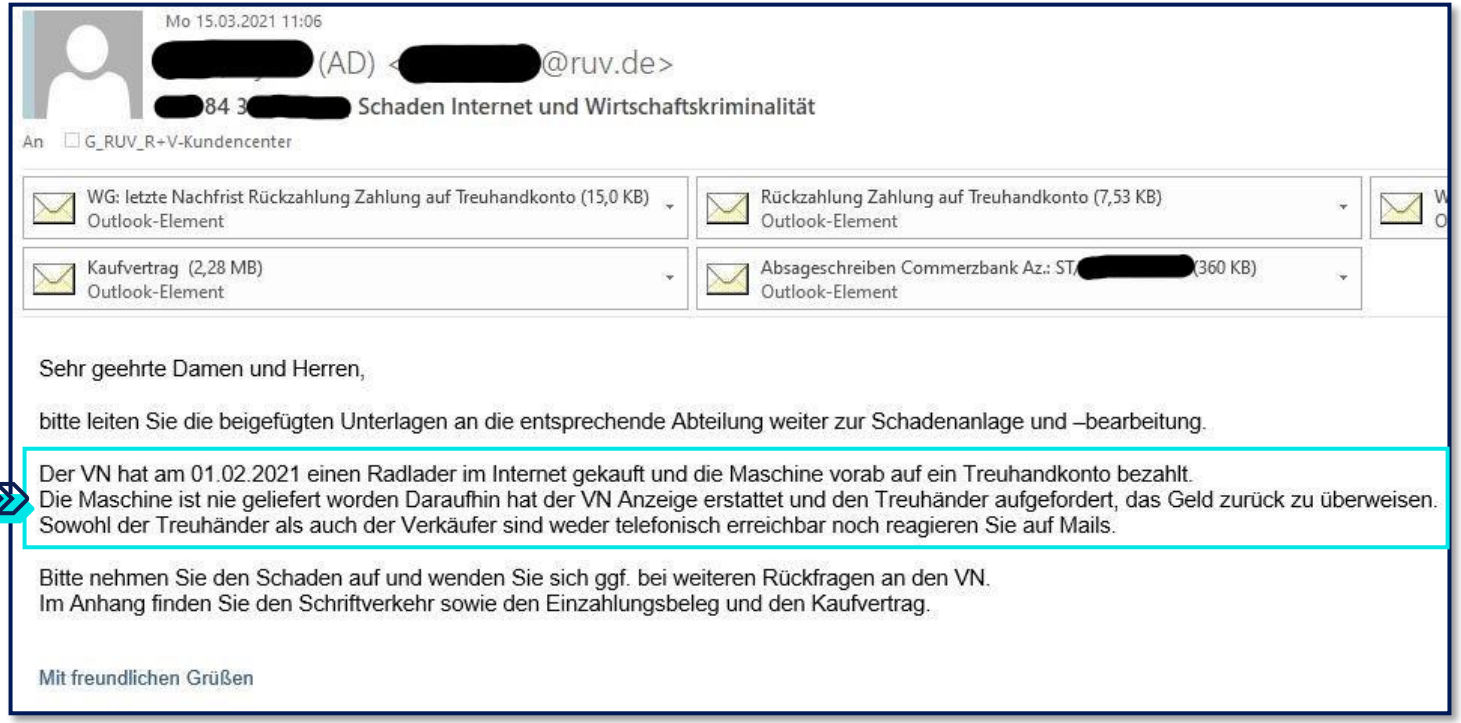
BSI - Deepfakes - Gefahren und Gegenmaßnahmen (bund.de)



Lieferbetrug

Betrüger geben sich als seriöse Verkäufer aus

Versicherungsnehmer → Handwerksbetrieb mit 14 Mitarbeitern aus dem Bereich Innenausbau



Mo 15.03.2021 11:06

[redacted] (AD) <[redacted]@ruv.de>

[redacted]84 3[redacted] Schaden Internet und Wirtschaftskriminalität

An G_RUV_R+V-Kundencenter

WG: letzte Nachfrist Rückzahlung Zahlung auf Treuhandkonto (15,0 KB)
Outlook-Element

Rückzahlung Zahlung auf Treuhandkonto (7,53 KB)
Outlook-Element

Kaufvertrag (2,28 MB)
Outlook-Element

Absageschreiben Commerzbank Az.: ST/[redacted] (360 KB)
Outlook-Element

Sehr geehrte Damen und Herren,

bitte leiten Sie die beigefügten Unterlagen an die entsprechende Abteilung weiter zur Schadenanlage und –bearbeitung.

Der VN hat am 01.02.2021 einen Radlader im Internet gekauft und die Maschine vorab auf ein Treuhandkonto bezahlt.
Die Maschine ist nie geliefert worden Daraufhin hat der VN Anzeige erstattet und den Treuhänder aufgefordert, das Geld zurück zu überweisen.
Sowohl der Treuhänder als auch der Verkäufer sind weder telefonisch erreichbar noch reagieren Sie auf Mails.

Bitte nehmen Sie den Schaden auf und wenden Sie sich ggf. bei weiteren Rückfragen an den VN.
Im Anhang finden Sie den Schriftverkehr sowie den Einzahlungsbeleg und den Kaufvertrag.

Mit freundlichen Grüßen

Überweisungsbetrug

Betrüger geben sich als bekannte Geschäftspartner aus

„Wir haben vier Zahlungen auf das Konto eines Betrügers überwiesen.
Es handelte sich um Zahlungen für einen indischen Meterwarenlieferanten,
zu welchem wir eine regelmäßige Geschäftsverbindung unterhalten.

Unser IT-Dienstleister analysierte die E-Mail Protokolle. Diese ergaben,
dass uns unter gefälschter Internet Absender ID eine falsche Bankverbindung mittgeteilt wurde.“

Überweisungsbetrug
Rückholung der Überweisung kaum möglich

„Die Banken haben wir am gleichen Tag nach Bekanntwerden des Betrugsfalls informiert und mit der Rückholung der Überweisungsbeträge beauftragt.

Es wurde uns mitgeteilt, dass die Chancen hierfür als gering bis aussichtslos eingestuft werden.

Somit gehen wir auch heute von einem 100%igen Verlust der Überweisungsbeträge aus.“

Schadenhöhe: 63.500 Euro

Warenbestellbetrug

Betrüger geben sich als vermeintliche Kunden aus

Von: T[redacted]
Datum: [redacted] Februar 2021 um 09:28:30 MEZ
An: [redacted] (AD)" <[redacted]@ruv.de>
Betreff: [redacted]

Guten Morgen Herr[redacted]

Wir haben bei Ihnen den Kunden [redacted] über die Warenkreditversicherung versichert

Jetzt ist folgendes passiert.

Es schein, als seien wir einem Wirtschaftsbetrug unterlegen

Zur Sache :

Wir haben Ihnen die uns vom Kunden zwecks Versicherung zur Verfügung gestellten Details überspielt. Der Kunde wurde versichert.
Wir erhielten die Bestellung des Kunden in Form der Rücksendung unserer vom Kunden unterschriebenen und gestempelten Auftragsbestätigung

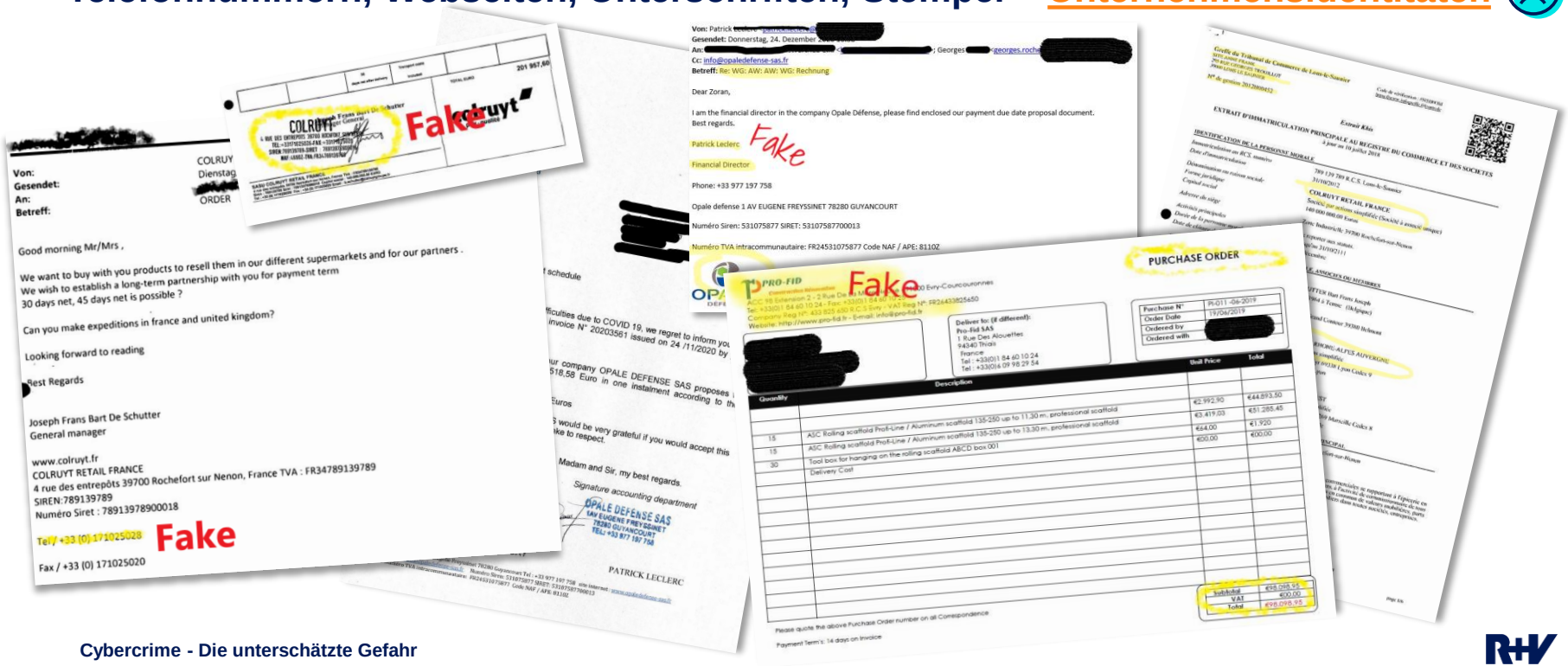
Soweit war für uns noch alles in Ordnung.

Wir haben alle Papiere gemäß dem Wunsch des Kunden in dessen Lagerhaus nach England in KW [redacted] 2021 vorgenommen und uns dann am [redacted] 21 nach der Zahlung erkundigt.

Soweit auch noch alles in Ordnung.

Identitätsdiebstahl und
Betrug wohin man schaut!

- **Perfekt gefälschte Auftragsdokumente, Handelsregisterauszüge, E-Mailadressen, Telefonnummern, Webseiten, Unterschriften, Stempel = Unternehmensidentitäten** ☹



IT-Sicherheit ist Chefsache

Ausgangssituation

Unsere Erfahrung aus zahlreichen Kundengesprächen!

Viele Unternehmen/Unternehmer

- unterschätzen die Gefahr durch Cyberrisiken,
- sind sich der Tragweite der DSGVO nicht bewusst und
- auf die damit verbundenen Haftungsrisiken nicht oder nicht ausreichend vorbereitet.

Wir können helfen!

R+V-Konzept IT-Sicherheit

Wesentliche Merkmale und Vorteile auf einen Blick:

- ✓ Schutz vor finanziellen Folgen bei Zerstörung, Beschädigung, Manipulation elektronischer Daten, z.B. durch Hacking, Phishing, Pharming, Trojaner, Schadcode, Identitätsdiebstahl, Datenmissbrauch, Daten-Diebstahl
- ✓ **Echte Soforthilfe im Schadenfall durch unser IT-Expertenteam**
- ✓ **Einzigartig am Markt: Allgefahren-Deckung**

R+V-Konzept IT-Sicherheit

Wesentliche Merkmale und Vorteile auf einen Blick:

- ✓ **Anwaltstelefon und freie Anwaltswahl**
- ✓ **Versicherungsschutz auch bei Vorwurf des Vorsatzes**
- ✓ **Auf Wunsch Vermittlung von Fachanwälten und IT-Spezialisten**

Wir kümmern uns um die Stärkung der IT-Sicherheit Ihres Unternehmens, damit Sie sich um Ihr Unternehmen kümmern können.

Wir können helfen!

CyCo-Trap
Die digitale Alarmanlage im 21. Jahrhundert

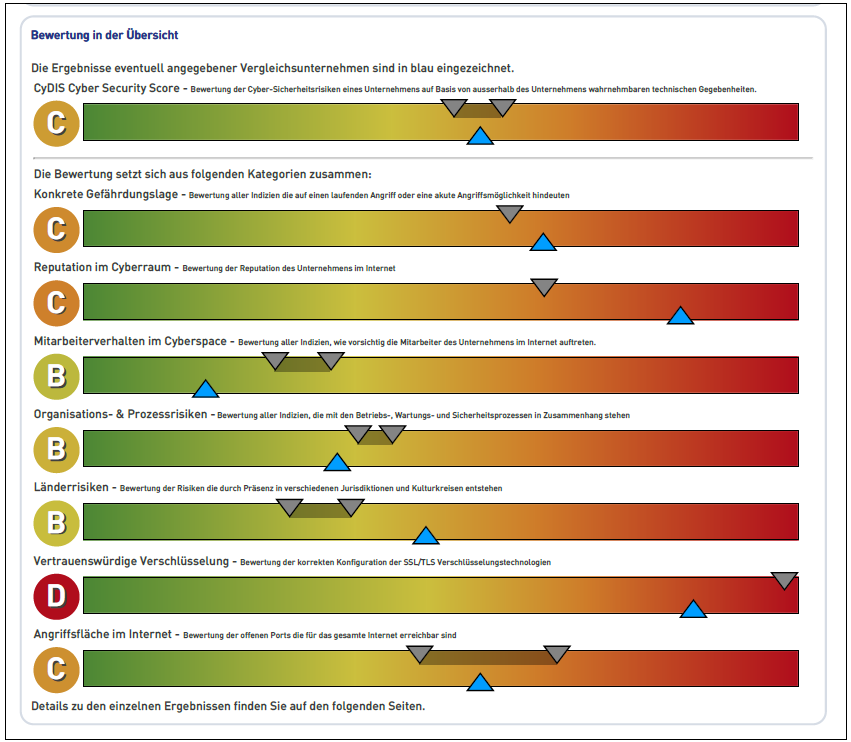
Leistungsspektrum

- CyCo-Trap erkennt Angreifer bevor sie Schäden anrichten
- Sofortige Alarmierung
- Wir schützen Ihre Daten! - Umleitung der Angreifer in fiktive virtuelle Umgebungen
- keine Wartungsarbeiten von Ihrer Seite
- Minimalster Installationsaufwand

Im ersten Jahr kostenfrei für R+V-CyberRisk Kunden

Cyber SecurityCheck

Auszug



Bewertung in der Übersicht

Die Ergebnisse eventuell angegebener Vergleichsunternehmen sind in blau eingezeichnet.

CyDIS Cyber Security Score – Bewertung der Cyber-Sicherheitsrisiken eines Unternehmens auf Basis von ausserhalb des Unternehmens wahrnehmbaren technischen Gegebenheiten.

C

Die Bewertung setzt sich aus folgenden Kategorien zusammen:

Konkrete Gefährdungslage – Bewertung aller Indizien die auf einen laufenden Angriff oder eine akute Angriffsmöglichkeit hindeuten

C

Reputation im Cyberraum – Bewertung der Reputation des Unternehmens im Internet

C

Mitarbeiterverhalten im Cyberspace – Bewertung aller Indizien, wie vorsichtig die Mitarbeiter des Unternehmens im Internet auftreten.

B

Organisations- & Prozessrisiken – Bewertung aller Indizien, die mit den Betriebs-, Wartungs- und Sicherheitsprozessen in Zusammenhang stehen

B

Länderrisiken – Bewertung der Risiken die durch Präsenz in verschiedenen Jurisdiktionen und Kulturkreisen entstehen

B

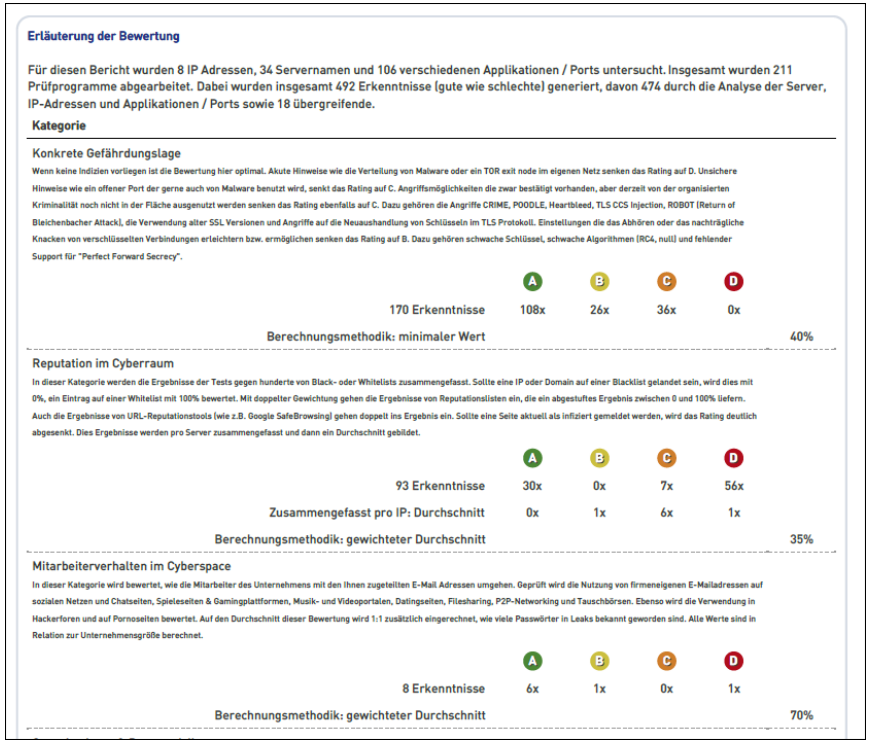
Vertrauenswürdige Verschlüsselung – Bewertung der korrekten Konfiguration der SSL/TLS Verschlüsselungstechnologien

D

Angriffsfläche im Internet – Bewertung der offenen Ports die für das gesamte Internet erreichbar sind

C

Details zu den einzelnen Ergebnissen finden Sie auf den folgenden Seiten.



Erläuterung der Bewertung

Für diesen Bericht wurden 8 IP Adressen, 34 Servernamen und 106 verschiedenen Applikationen / Ports untersucht. Insgesamt wurden 211 Prüfprogramme abgearbeitet. Dabei wurden insgesamt 492 Erkenntnisse (gute wie schlechte) generiert, davon 474 durch die Analyse der Server, IP-Adressen und Applikationen / Ports sowie 18 übergreifende.

Kategorie

Konkrete Gefährdungslage

Wenn keine Indizien vorliegen ist die Bewertung hier optimal. Akute Hinweise wie die Verteilung von Malware oder ein TOR exit node im eigenen Netz senken das Rating auf D. Unsichere Hinweise wie ein offener Port der gerne auch von Malware benutzt wird, senkt das Rating auf C. Angriffsmöglichkeiten die zwar bestätigt vorhanden, aber derzeit von der organisierten Kriminalität noch nicht in der Fläche ausgenutzt werden senken das Rating ebenfalls auf C. Dazu gehören die Angriffe CRIME, POODLE, Heartbleed, TLS CCS Injection, ROBOT (Return of Bleichenbacher Attack), die Verwendung alter SSL Versionen und Angriffe auf die Neuaushandlung von Schlüsseln im TLS Protokoll. Einstellungen die das Abhören oder das nachträgliche Knacken von verschlüsselten Verbindungen erleichtern bzw. ermöglichen senken das Rating auf B. Dazu gehören schwache Schlüssel, schwache Algorithmen (RC4, null) und fehlender Support für "Perfect Forward Secrecy".

	A	B	C	D	
170 Erkenntnisse	108x	26x	36x	0x	
Berechnungsmethodik: minimaler Wert					40%

Reputation im Cyberraum

In dieser Kategorie werden die Ergebnisse der Tests gegen hunderte von Black- oder Whitelists zusammengefasst. Sollte eine IP oder Domain auf einer Blacklist gelandet sein, wird dies mit 0%, ein Eintrag auf einer Whitelist mit 100% bewertet. Mit doppelter Gewichtung gehen die Ergebnisse von Reputationslisten ein, die ein abgestuftes Ergebnis zwischen 0 und 100% liefern. Auch die Ergebnisse von URL-Reputationstools (wie z.B. Google SafeBrowsing) gehen doppelt ins Ergebnis ein. Sollte eine Seite aktuell als infiziert gemeldet werden, wird das Rating deutlich abgesenkt. Dies Ergebnisse werden pro Server zusammengefasst und dann ein Durchschnitt gebildet.

	A	B	C	D	
93 Erkenntnisse	30x	0x	7x	56x	
Zusammengefasst pro IP: Durchschnitt	0x	1x	6x	1x	
Berechnungsmethodik: gewichteter Durchschnitt					35%

Mitarbeiterverhalten im Cyberspace

In dieser Kategorie wird bewertet, wie die Mitarbeiter des Unternehmens mit den Ihnen zugeteilten E-Mail Adressen umgehen. Geprüft wird die Nutzung von firmeneigenen E-Mailadressen auf sozialen Netzen und Chatseiten, Spieleseiten & Gamingplattformen, Musik- und Videoportalen, Datingseiten, Filesharing, P2P-Networking und Tauschbörsen. Ebenso wird die Verwendung in Hackerforen und auf Pornoseiten bewertet. Auf den Durchschnitt dieser Bewertung wird 1:1 zusätzlich eingerechnet, wie viele Passwörter in Leaks bekannt geworden sind. Alle Werte sind in Relation zur Unternehmensgröße berechnet.

	A	B	C	D	
8 Erkenntnisse	6x	1x	0x	1x	
Berechnungsmethodik: gewichteter Durchschnitt					70%

IT-Sicherheit ist Chefsache

Wir können helfen

3 Fragen an Sie:

- ✓ **Montagmorgen, etwa 07:47 Uhr: Bildschirm schwarz, kein Zugriff auf Daten mehr möglich. Telefon und Fax „tot“. Was ist Ihnen jetzt wichtig?**
- ✓ **Wie haben Sie sichergestellt, dass Sie einen Cyber-Angriff finanziell unbeschadet überstehen?**
- ✓ **Wie haben Sie Ihre berufliche Haftung als Geschäftsführer/ Inhaber/ Chef in Folge eines Sicherheitsvorfalls abgesichert?**