Symposium des DStV-Verbändeforums IT in Berlin
Born to protect

Dieter Schröter, Internet-Security DATEV eG

Fürther Klinikum Finanzamt Security

Tückischer Virus

Noch kein Ende: EMOTET birgt weiter Gefahren fürs Fürther Klinikum.

FÜRTH. Das IT-Netz des Berliner Kammergerichts wurde bereits im September infiziert. Seitdem ist das Computersystem vom Internet abgekoppelt, Mitarbeiter können ihre Rechner nur noch als Schreibmaschinen nutzen, berichtet etwa die Nachrichtenseite *heise online*. Technisch sei man auf einem Stand wie vor 30 Jahren. Und man geht davon aus, dass der Notbetrieb erst 2020 endet.

Die Uni Gießen, die ebenfalls schwer vom gefährlichen Trojaner Emotet getroffen wurde, hat in diesen Tagen 28 000 neue Passwörter an ihre Studenten verteilt – sie waren in der Turnhalle abzuholen, es bildeten sich Schlangen. Es könnte Wochen dauern, bis der Hochschulalltag wieder wie gewohnt läuft.

Auch am Fürther Klinikum wird die IT-Attacke die IT-Experten noch wochenlang beschäftigen, sagt Kliniksprecher René Icgen. Was Emotet so gefährlich macht: Sind Rechner einmal infiziert, können Kriminelle weitere Schadsoftware nachladen – darunter den Banking-Trojaner Trickbot, der Kontos knacken soll, oder Programme, die Dateien verschlüsseln und Lösegeld fordern, um sie wieder nutzbar zu machen. Auch Privatanwender können wichtige Daten, etwa Zugangsdaten, verlieren.

Am Klinikum arbeiten die Experten Icgen zufolge nun rund um die Uhr daran, die IT-Struktur vor Folgeangriffen zu schützen. Bisher gebe es keine Indizien dafür, dass Daten abgewandert seien. Auch die Versorgung der Patienten sei stets gewährleistet geblieben, medizinische Geräte funktionierten weiter. Stark eingeschränkt ist dagegen die digitale Kommunikation der Mitarbeiter.

Emotet macht bundesweit bereits seit dem Herbst PCs und Datennetzwerke unsicher. Die Methoden sind hochprofessionell, sagt das Bundesamt für Sicherheit in der Informationstechnik (BSI). Über verseuchte Anhänge und Links können Bürger ihre Computer infizieren.

Das Tückische: Auf den ersten Blick wirken die Absender vertraut. Emotet kann Mail-Inhalte der zurückliegenden Wochen auslesen – die fatale Mail scheint an einen vorhergehenden Mailverkehr anzuknüpfen. Fachleute raten dazu, sich die Absenderadresse genau anzusehen. Tauchen dort kryptische Zeichen auf, ist höchste Vorsicht angeraten. Im Zweifel sollte man telefonisch mit dem vermeintlichen Absender klären, ob die Mail wirklich von ihm stammt.

Besondere Vorsicht sollte man bei E-Mails mit Dateianhang oder Links walten lassen. Der Virus arbeitet auch mit Office-Dokumenten, er lauert zum Beispiel in angeblichen Rechnungen im .doc-Format. **czi/tig**

Quelle: Bad Windsheimer Zeitung 21./22. 12 2019

Süddeutsche Zeitung

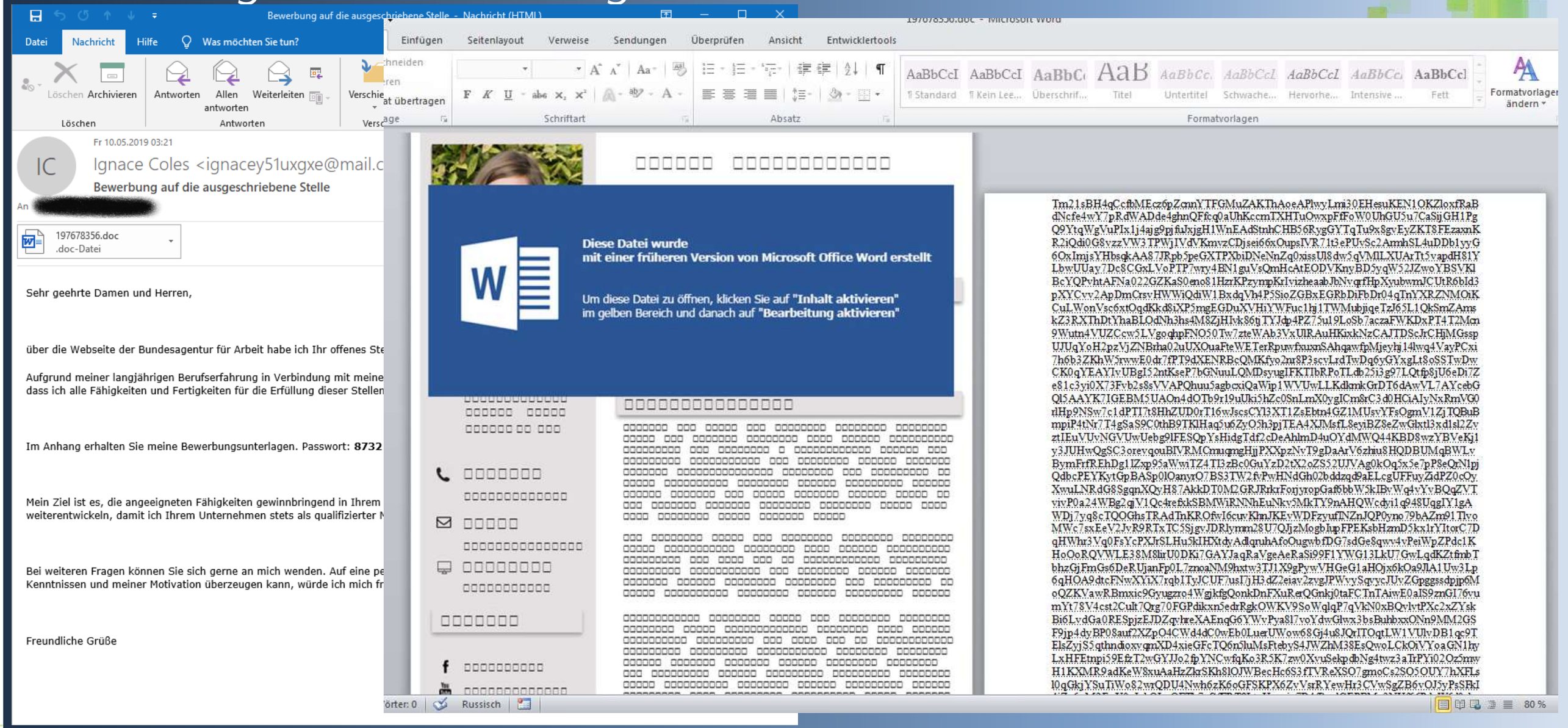
SZ.de Zeitung Magazin

8. Januar 2020, 19:54 Uhr Finanzen - Hannover

Schadsoftware: E-Mail-Verkehr mit Finanzämtern eingeschränkt

Hannover (dpa/lni) - Aufgrund der verschärften Bedrohungslage durch die Schadsoftware "Emotet" ist der E-Mail-Verkehr mit den niedersächsischen Finanzämtern erheblich eingeschränkt. Betroffen seien E-Mails, die von außerhalb des Landesnetzes an die Finanzverwaltung gerichtet sind und MS-Office-Anhänge wie zum Beispiel Word-Dokumente enthalten, teilte das Finanzministerium am Mittwoch in Hannover mit. Gleiches gelte für mit einem Hyperlink versehene E-Mails, die durch Anklicken auf eine Webseite führten. Für Steuerberater sowie Nutzer der Steuersoftware "Elster" gibt es den Angaben zufolge aber keine Einschränkungen. Die Abgabe von Steuererklärungen über "Elster" sei weiterhin möglich, hieß es. Auch Steuerberater-Software wie Datev funktioniere. Die Sicherheitsmaßnahmen würden fortlaufend überprüft. Derzeit sei nicht abzusehen, wann sie wieder heruntergefahren werden könnten.

Phishing – Awareness -gandcrab



Phishing – Awareness –GandCrab geht in Rente

Security 〉7-Tage-News 〉06/2019 〉**Erpressungstrojaner GandCrab geht offenbar in Rente**

heise online

Erpressungstrojaner GandCrab geht offenbar in Rente

Die Malware-Entwickler von GandCrab haben das Ende der Kampagne bekannt gegeben. Eigenen Angaben zufolge haben sie pro Woche 2,5 Millionen US-Dollar verdient.

03.06.2019 13:55 Uhr | Security

Von Dennis Schirrmacher

Der Verschlüsselungstrojaner GandCrab hat seit Anfang 2018 Windows-Computer infiziert, Dateien verschlüsselt und Lösegelder eingefordert. Nun ist damit offenbar Schluss: Die Entwickler der Ransomware haben im Malware-Forum Exploit.in das Ende von GandCrab bekannt gegeben. Das berichten mehrere Sicherheitsforscher auf Twitter.

Eigenen Angaben zufolge haben Opfer Lösegelder in Höhe von insgesamt mehr als 2 Milliarden US-Dollar an die Kriminellen gezahlt, um so die Schlüssel für ihre Daten zu bekommen. Die Entwickler geben an, mit ihrer Masche pro Woche 2,5 Millionen US-Dollar verdient zu haben. Pro Jahr waren es 150 Millionen US-Dollar. Das Geld haben sie dem Statement zufolge in verschiedene legale Projekte investiert.

https://www.heise.de/security/meldung/Erpressungstrojaner-GandCrab-geht-offenbar-in-Rente-4437046.html

Wie viel Malware gibt es?

144,89 Mio 2019

AV-TEST The Independent IT-Security Institute

Quelle: www.av-test.org

Dashboard
Aktuelle Bedrohungen
Tools
Blackhat URLs
Spam
Flare Whitelist

AV-ATLAS analysiert für Sie:

Mails in der letzten Woche
55.172
19% weniger als in der Vorwoche

Mails mit Links in der letzten Woche
44.231
25% weniger als in der Vorwoche

Indizierte URLs
553.595
In den letzten 48 Stunden

Letzte Erkennung
FlyStudio
vor einer Stunde

Die aktuelle Bedrohungslage im Überblick:

GEFÄHRLICHER TREND

Vermeiden Sie den Suchbegriff **Legends of Tomorrow torrent**!
AV-TEST hat kürzlich **6 gefährliche** Suchergebnisse zu diesem Begriff gefunden!

Weitere gefährliche Trends

GEFÄHRLICHE PHISHINGMAILS

AV-TEST hat kürzlich **14** Phishingmails mit dem Betreff **DROPS X SIZES FROM YOUR WAIST SHARK TANK** gefunden!
Öffnen Sie keine Links oder Anhänge solcher Mails und geben Sie nie Passwörter in Webseiten, auf welche diese Mails weiterleiten, ein!

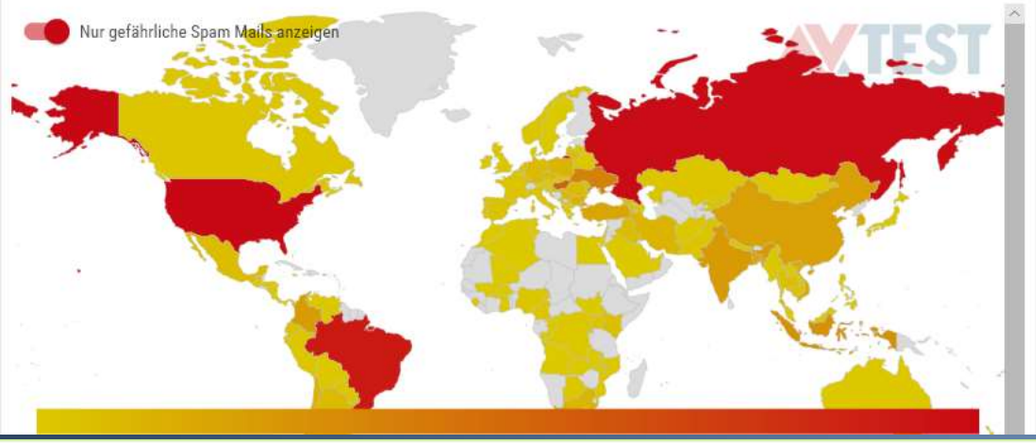
Weitere Trends zu E-Mailbetreffen

NEUE ERPRESSUNGSMAILS

AV-TEST hat kürzlich **42** erpresserische E-Mails mit dem Betreff **MESSAGE SUBJECT** gefunden!
Öffnen Sie keine Links oder Anhänge solcher Mails und erfüllen Sie niemals Zahlungsaufforderungen solcher Mails!

Weitere Trends zu E-Mailbetreffen

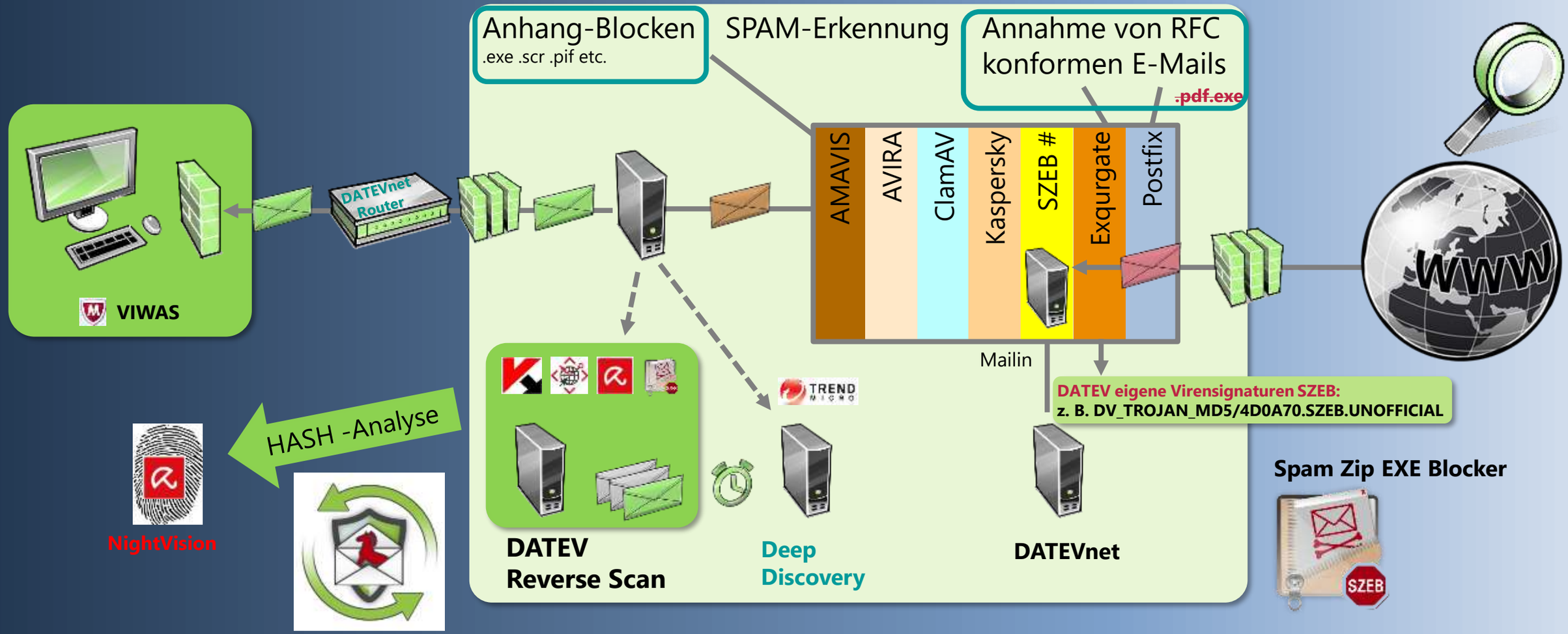
HERKUNFT VON SPAM-MAILS



INDIZIERTE, ANALYSIERTE UND VERDÄCHTIGE URLS

MEHR DATEN?
Kontaktieren Sie uns!

DATEV - DATEVnet
E-Mail-Schutz



SZEB – Virenschutz – Reaktion
Erfolg – dv_Trojan_md5/02f69d.szeb.UNOFFICIAL

SZEB – 5.945 – mit einem eigenen Pattern geblockt

Betreff: „Retourenlabel zu Ihrer DHL Sendung 9381048598“
Anhang: „Ihre Retourenmarke.zip“

- **15:20 Uhr** – Trojaner-Welle prasselt auf DATEV ein
- 15:22 Uhr – SZEB-Pattern – automatisiert (dv_Trojan_md5/02f69d.szeb.UNOFFICIAL)

- 15:30 Uhr – Viren Sample an alle AV-Hersteller
- **16:39 Uhr** – Trojaner-Welle ist beendet

Feedback AV-Hersteller

- 17:10 Uhr
  - Kaspersky
  - Avira
  - McAfee

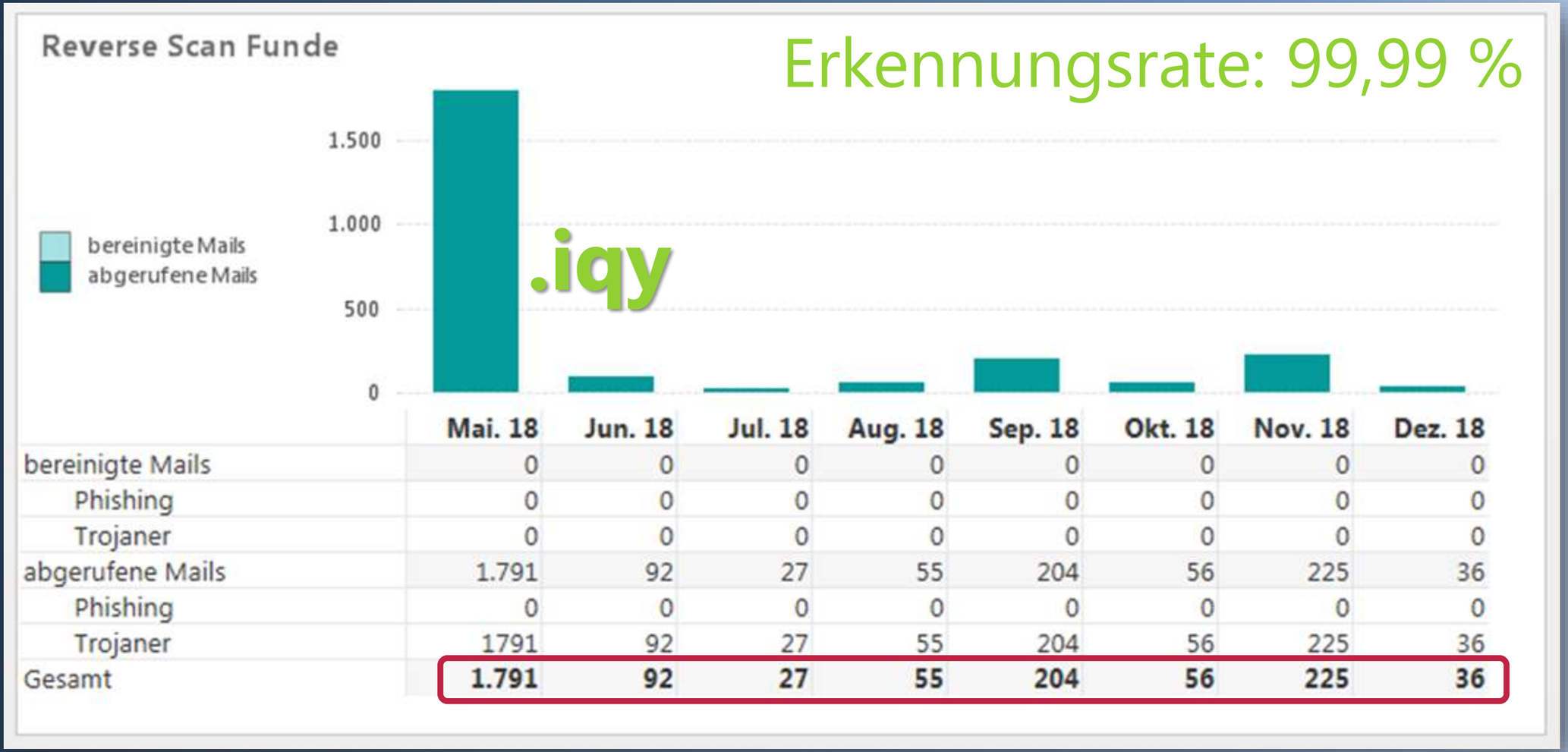
Highlights

- stärkster Tag: 1.546 SZEB-Pattern
- stärkster Monat: 19.461 SZEB-Pattern
  65.015 Funde

DATEVnet Sicherheit
Kennzahlen E-Mail

	Mai. 19	Jun. 19	Jul. 19	Aug. 19	Sep. 19	Okt. 19	Nov. 19	Dez. 19
zugestellt	14.694	12.998	15.167	14.299	15.053	16.095	15.976	15.023
Spam	556	493	637	626	709	699	570	750
nicht zugestellt	2.595	2.685	3.144	3.177	3.977	3.699	3.068	3.772
Gesamt *	**17.289**	**15.683**	**18.311**	**17.476**	**19.030**	**19.795**	**19.044**	**18.795**
Viren	270	265	187	132	249	210	122	71
Spam	1.151	1.260	1.487	1.597	2.039	1.708	1.239	1.286
Greylisting	1.175	1.160	1.470	1.448	1.689	1.782	1.708	2.415
Gesamt *	**2.595**	**2.685**	**3.144**	**3.177**	**3.977**	**3.699**	**3.068**	**3.772**

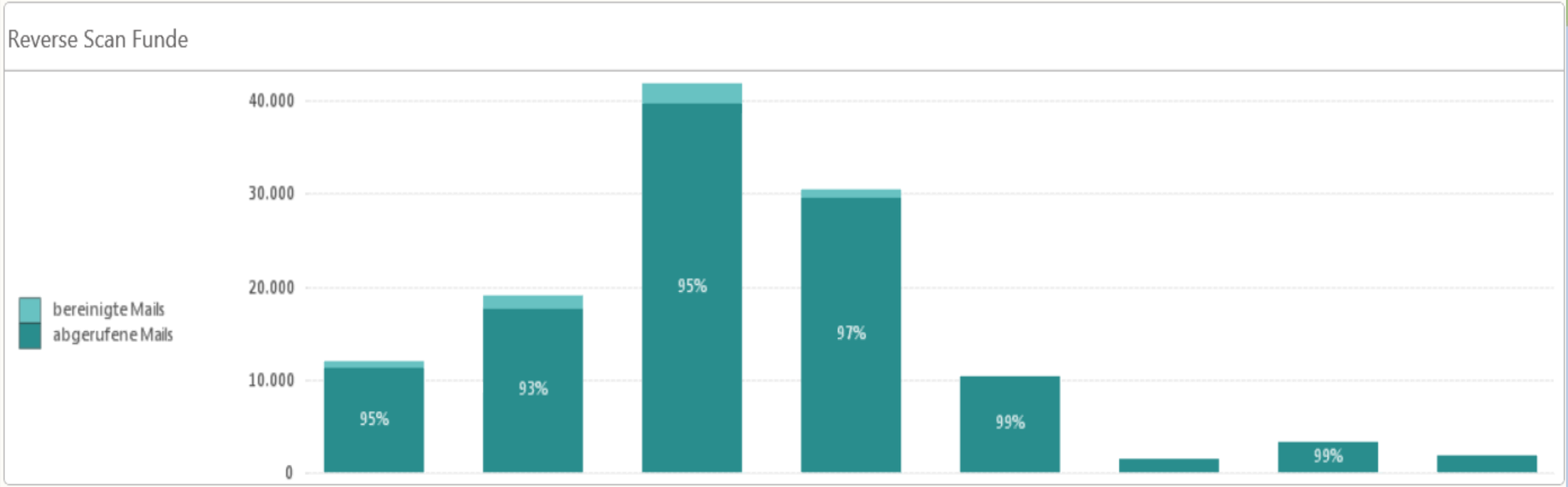
DATEVnet Sicherheit – Reverse Scan Funde



	Mai. 18	Jun. 18	Jul. 18	Aug. 18	Sep. 18	Okt. 18	Nov. 18	Dez. 18
bereinigte Mails	0	0	0	0	0	0	0	0
Phishing	0	0	0	0	0	0	0	0
Trojaner	0	0	0	0	0	0	0	0
abgerufene Mails	1.791	92	27	55	204	56	225	36
Phishing	0	0	0	0	0	0	0	0
Trojaner	1791	92	27	55	204	56	225	36
Gesamt	**1.791**	**92**	**27**	**55**	**204**	**56**	**225**	**36**

QS → Continual Service Improvement

Reverse Scan Funde 2012–2019



	2012	2013	2014	2015	2016	2017	2018	2019
bereinigte Mails	600	1.318	2.127	930	115	39	29	38
Phishing	1	3	32	2	0	0	0	0
Trojaner	599	1315	2095	928	115	39	29	38
abgerufene Mails	11.292	17.610	39.695	29.566	10.267	1.373	3.211	1.760
Phishing	108	94	1.222	148	49	29	0	0
Trojaner	11184	17516	38473	29418	10218	1344	3211	1760
Gesamt	**11.892**	**18.928**	**41.822**	**30.496**	**10.382**	**1.412**	**3.240**	**1.798**

Strategie – Security Thinking
Security Lifecycle


PROTECTION
REACTION
DETECTION

CERTIFICATE

av-test.org

Tested Company

DATEV

Tested Security Layer

Corporate E-Mail Security

In a long-term project, the AV-TEST institute monitored the corporate e-mail security systems. We performed real-time tests with live and confirmed malicious e-mails and spam to gather long-term data. The results prove that the e-mail security implementation is capable of effectively securing a corporate network. Therefore, the AV-TEST institute awards the seal for "Monitored Corporate E-Mail Security".

MONITORED CORPORATE E-MAIL SECURITY
11/2018

Magdeburg, 1st November 2018

Andreas Marx
Chief Executive Officer (CEO)

Guido Habicht
Chief Executive Officer (CEO)

Maik Morgenstern
Chief Technology Officer (CTO)

Postal address: Klewitzstr. 7, 39112 Magdeburg, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69
For further details, please visit: https://www.av-test.org

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

ZERTIFIKAT

Hiermit wird bescheinigt, dass

DATEV eG
Paumgartnerstraße 6-14
90429 Nürnberg
Deutschland

ein **Informationssicherheits-Managementsystem**
eingeführt hat und anwendet.

Geltungsbereich:
DATEV Rechenzentrum inklusive DATEVnet sowie Dienstleistungen des DATEV Druck-, Logistik- und Servicezentrums für interne und externe Kunden inclusive des digitalen Scannens

Erklärung zur Anwendbarkeit: V4.3

Durch ein Audit, dokumentiert in einem Bericht, wurde der Nachweis erbracht, dass das Managementsystem die Forderungen des folgenden Regelwerks erfüllt:

ISO / IEC 27001 : 2013

Zertifikat-Registrier-Nr.	337181 ISMS13
Gültig ab	2019-12-19
Gültig bis	2022-12-18
Zertifizierungsdatum	2019-12-19

DAkkS Deutsche Akkreditierungsstelle D-ZM-16074-01-00

DQS GmbH

Markus Bleher
Geschäftsführer

Akkreditierte Stelle: DQS GmbH, August-Schanz-Straße 21, 60433 Frankfurt am Main
Administrative Stelle: DQS BIT GmbH, Gartenäckerstraße 13, 86825 Bad Wörishofen

Bewerbungsunterlagen-Schumacher (Geschützte Ansicht) - Microsoft Word

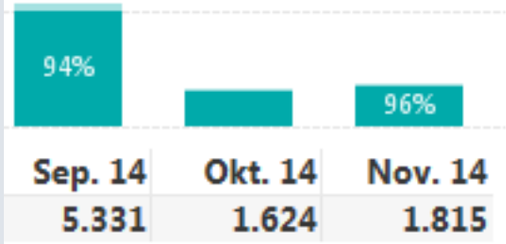
Datei Start Einfügen Seitenlayout Verweise Sendungen Überprüfen Ansicht

Geschützte Ansicht Diese Datei stammt von einem Internetspeicherort und kann ein Risiko darstellen. Klicken Sie hier, um weitere Details anzuzeigen. Bearbeitung aktivieren

Bewerbungsmappe von Simon Schumacher

Seite: 1 von 9 Wörter: 121 75 %

14.931 Spam = yes
945 Spam = no



Schützen die Gesetze Spam?

Verletzung des Post- oder Fernmeldegeheimnis –
unterdrücken anvertrauter Sendungen

- Zustellgebot (auch für die „Bösen“)
- E-Mail-Adresse muss erreichbar sein
- geschäftlicher Spamordner muss täglich kontrolliert werden (siehe Urteil – Heise vom 15.07.2014)

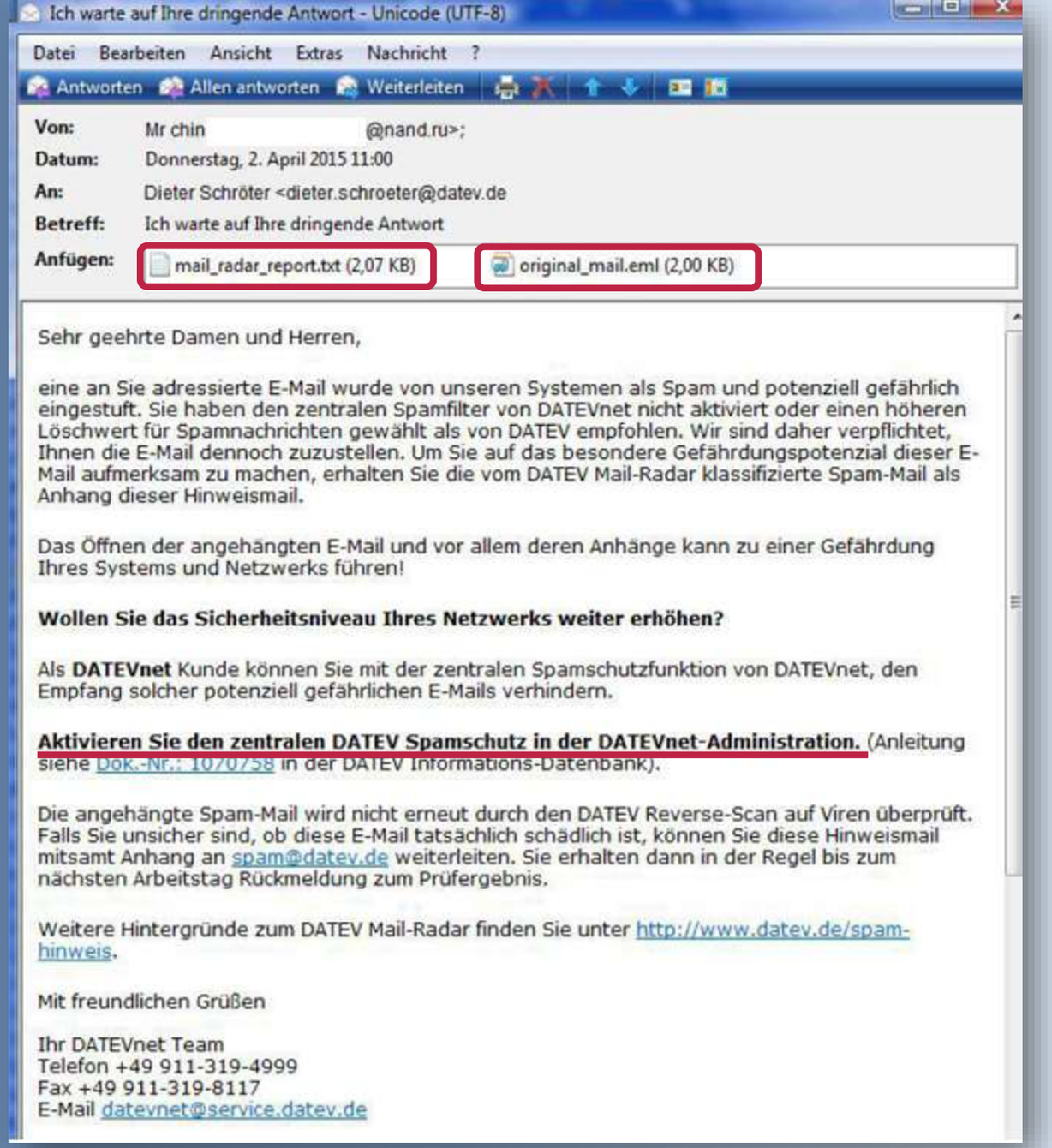
Lösung: Spam-Filter DATEVnet aktivieren
(DATEV-Legal → OK)

Spam = dangerous

E-Mail-Radar aktiv seit 02/2015

DATEV Mail-Radar
Wie geht das?

- **Original-Mail** im Anhang
- **Mail-Radar-Report** im Anhang
- **Spam-Header** der Original-Mail
- **Filter-Regeln** greifen weiterhin
- **Spam-Filter** einschalten – **Bitte**
- **> 1000** Kunden aktivieren Spam-Filter
- **> 67.849** reduzierte Reverse Scan Funde



Bewerbung – Jobbörse

Betreff: Bewerbung als Lohn- und Gehaltsbuchhalter

Bewerbung als Lohn- und Gehaltsbuchhalter

Sehr geehrter Herr Erich

da ich auf der Suche nach einer neuen beruflichen Herausforderung bin, möchte ich mich hiermit bei Ihnen um eine Stelle als Lohn- und Gehaltsbuchhalter 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.

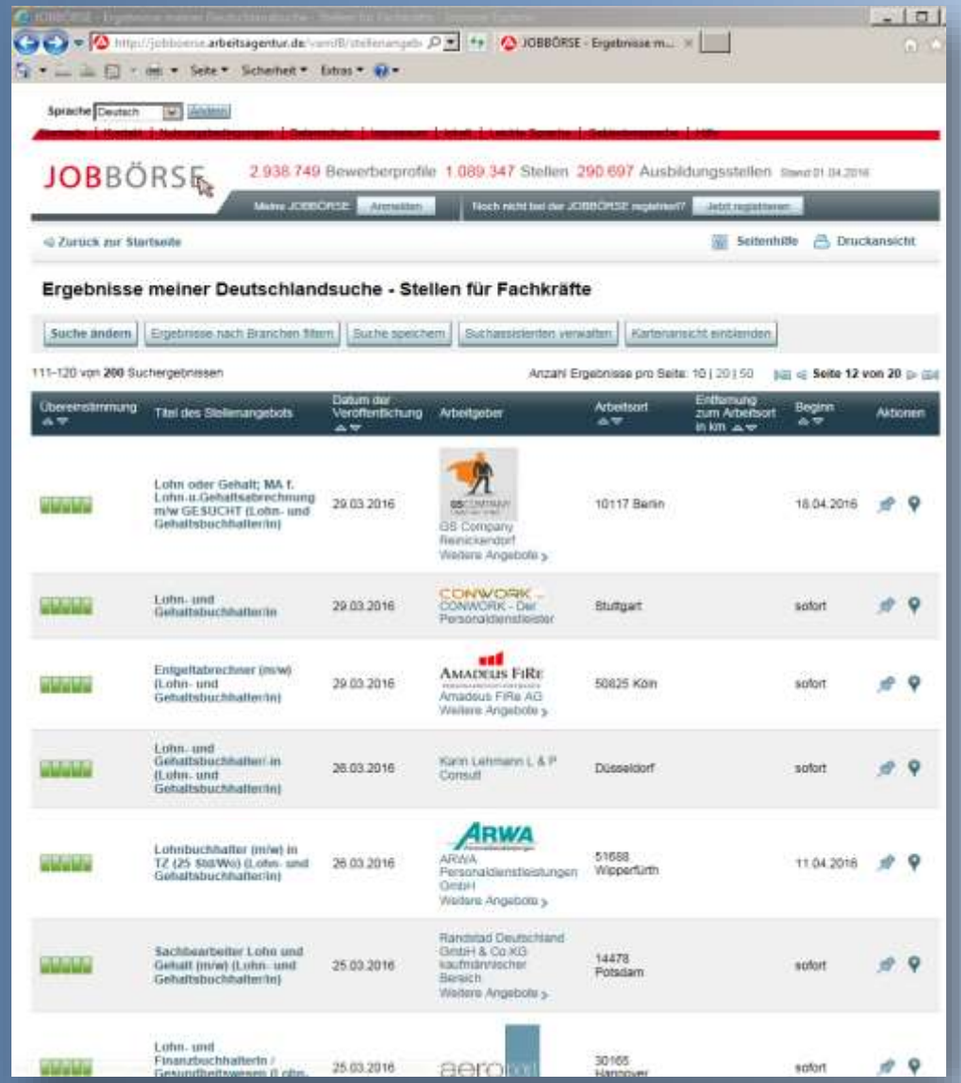
Mit freundlichen Grüßen

Kai

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/nfs6pmoq42hmn7w/AAB8 Tuiema?dl=0

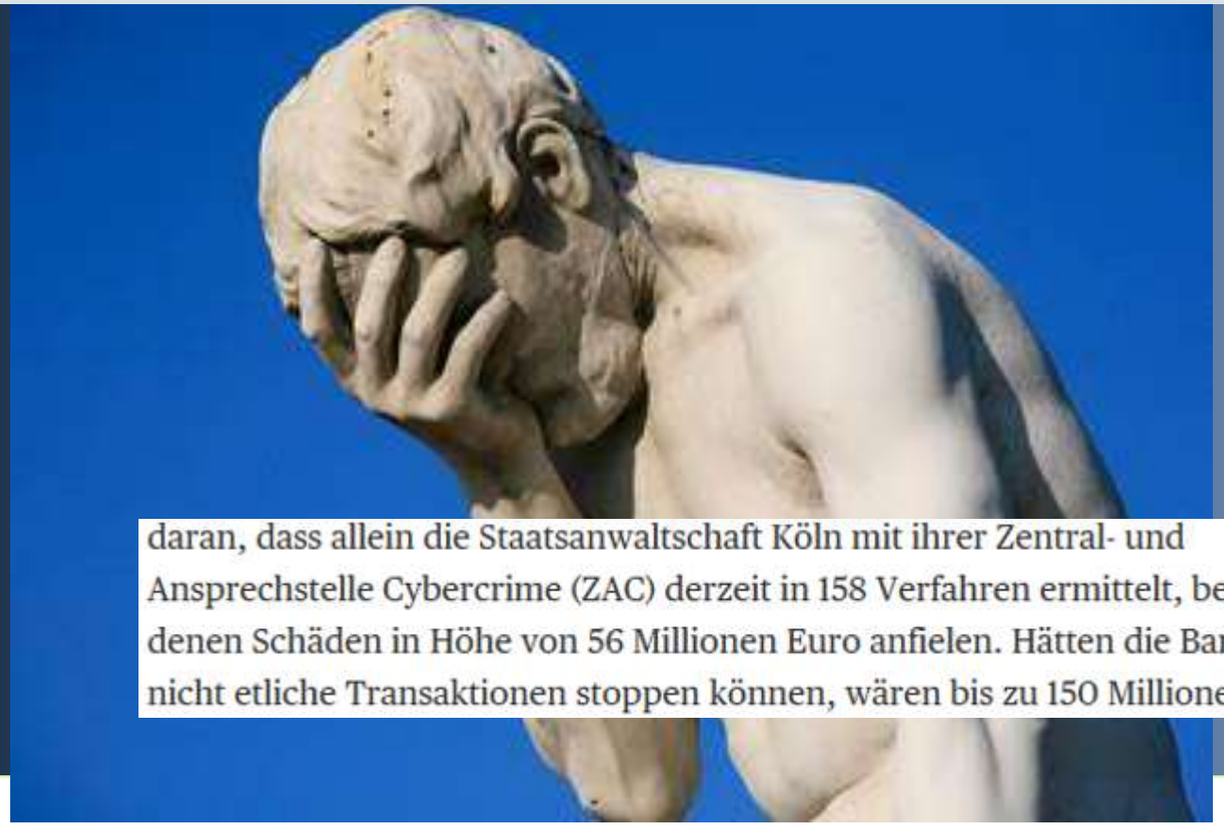


Quelle: www.arbeitsagentur.de Windsheimer

Business Security
CEO Fraud

Schadenswirkung: Angaben des Bundeskriminalamts zufolge wurden seit 2013 in Deutschland bisher 250 Betrugsfälle bekannt. Davon waren 68 erfolgreich, 182 blieben im Versuchsstadium stecken. Der Gesamtschaden betrage demnach 110 Millionen Euro.

Da der Betrug in manchen Fällen erst nach mehreren Tagen entdeckt wird und die Kriminellen die Überweisung im Ausland rasch weiterleiten, ist das Geld bei einer getätigten Überweisung oft unwiederbringlich verloren.



daran, dass allein die Staatsanwaltschaft Köln mit ihrer Zentral- und Ansprechstelle Cybercrime (ZAC) derzeit in 158 Verfahren ermittelt, bei denen Schäden in Höhe von 56 Millionen Euro anfielen. Hätten die Banken nicht etliche Transaktionen stoppen können, wären bis zu 150 Millionen

Mittwoch, 17. August 2016

Wurde Leoni Opfer der „Chef-Masche“?

Nürnberger Autozulieferer verlor 40 Mio. € – Betrüger nutzten gefälschte Papiere

VON MARKUS HACK

NÜRNBERG – Seit Monaten sorgt der Nürnberger Autozulieferer Leoni immer wieder für Schlagzeilen: Losgegangen ist das Elend im vergangenen Jahr, als vier neue Projekte in Rumänien wegen schwerer Managementfehler für hohe Verluste sorgten. Das weltweit agierende Unternehmen reagierte darauf im Frühjahr mit einem Maßnahmenbündel inklusive Stellenabbau auch in Deutschland. Im Juli gab dann der für die Problemsparte Bordnetze verantwortliche Vorstand Frank Hiller überraschend seinen Posten auf.

Und jetzt auch noch das: Der einst erfolgsverwöhnte Konzern geht Kriminellen auf den Leim. Die Betrüger transferierten – ohne dass intern rechtzeitig die Alarmglocken schrillten – 40 Mio. € auf Konten im Ausland, wie Leoni am Dienstag in einer Pflichtmitteilung bekanntgab. Man sei „Opfer betrügerischer Handlungen unter Verwendung gefälschter Dokumente und Identitäten sowie Nutzung elektronischer Kommunikationswege“ geworden.

Zu Details wollte sich das Unternehmen nicht äußern. Die Beschreibung des Betrugs passt aber auf die sogenannten Chef-Masche, vor der Anfang Juli das Landeskriminalamt Nordrhein-Westfalen bundesweit gewarnt hatte.

Die Methode: Ein Mitarbeiter in der Buchhaltung erhält eine Nachricht angeblich von oberster Stelle im Unternehmen und wird um Hilfe in einer diskreten Angelegenheit gebeten, wie etwa dem Kauf von Firmenanteilen oder Immobilien. Dafür müsse schnell Geld ins Ausland überwiesen werden. Die Betrüger halten vorbereitete Zahlungsaufträge bereit, die die jeweils notwendige zweite Unterschrift schon beinhalten. Diese ist jedoch gefälscht.

Hinter der kriminellen Masche soll ein global operierendes Netzwerk der organisierten Kriminalität stecken. Nach Angaben des amerikanischen FBI liegt der Schaden weltweit bei 3,1 Mrd. Dollar (2,8 Mrd. €). In Deutschland summierte sich der Schaden nach Angaben des Bundeskriminalamtes seit 2013 auf 106 Mio. €. Der Industrie- und Handelskammer Nürnberg für Mittelfranken sind derweil keine weiteren aktuellen Betrugsfälle bei anderen Unternehmen bekannt, hieß es dort.

Leoni zufolge hat der Konzernvorstand eine Untersuchung der Vorfälle eingeleitet, die intern am Freitag erkannt worden waren. Zugleich werden Schadenersatz- und Versicherungsansprüche geprüft. Zudem habe der Konzern Anzeige erstattet, hieß es. Bei der Polizei war diese gestern Nachmittag jedoch noch nicht eingegangen, sagte ein Sprecher des Polizeipräsidiums Mittelfranken auf Nachfrage.

Aktie sackte ab

Unklar ist nach Angaben des fränkischen Konzerns, wie stark sich der Betrug auf das Jahresergebnis auswirkt. Wegen der laufenden Sanierungsmaßnahmen hat Leoni ohnehin bereits angekündigt, dass das Ergebnis vor Steuern und Abschreibungen von zuvor 151 Mio. € auf heuer 105 Mio. € sinken werde. Die Aktie der im MDax notierten Gesellschaft verlor bis Handelsschluss um über sechs Prozent.

Quelle: Bad Windsheimer Zeitung

Business Security warnt Kunden

DATEVnet unterstützt Sie

Derzeit werden auch DATEVnet-Kunden per E-Mail aufgefordert, größere Geldsummen zu transferieren. Diese E-Mails wurden individuell verfasst und sind damit technisch kaum von normalen E-Mails zu unterscheiden. Falls Sie E-Mails mit Kontonummern erhalten, die Sie zu Überweisungen anhalten, nehmen Sie telefonisch Rücksprache mit dem vermeintlichen Absender. Verwenden Sie nicht die Mail-Funktion "Antworten".

14. Juli 2017, 07:41 Uhr Prozess

Buchhalterin der Hofpfisterei überweist 1,9 Millionen Euro an Trickbetrüger

Eine Buchhalterin der Hofpfisterei ist auf Trickbetrüger aus China reingefallen und hat 1,9 Millionen Euro nach Hongkong überwiesen.

Quelle: https://www.sueddeutsche.de/muenchen/prozess-buchhalterin-der-hofpfisterei-ueberweist-millionen-euro-an-trickbetrueger-1.3586564

Wertschöpfung aus Internetbedrohungen IBAN-Reputation

Von: .DE Deutsche Domain [mailto:kontakt14@deutschedomain.com]
Gesendet: Montag, 26. Oktober 2015 17:03
An: .DE Deutsche Domain
Betreff: Domainregistrierung 2015 / 2016
Wichtigkeit: Hoch

Sehr geehrte Frau / Herr,

Nachfolgend die Einzelheiten zu der Domainregistrierung für 2015 / 2016.

Wir hoffen, Sie ausreichend informiert zu haben.

Mit freundlichen Grüssen

Birgit

Kundendienst
DE Deutsche Domain
info@deutschedomain.com<mailto:info@deutschedomain.com>

.DE Deutsche Domain

Rechnung

.DE Deutsche Domain
info@deutschedomain.com
Kundendienst 0049-30 203 39
Deutschland

Rechnungsnummer	832101
Rechnungsdatum	26.10.2015
Zahlungsbedingungen	14 Tage
Rechnungskontakt	Birgit Hoffmann

Gesamt	**161,90 €**
Fälligkeitsdatum	09.11.2015
Ref.-Nr.	832101
IBAN:	ES7820389788336000165285
SWIFT / BIC:	CAHMESMMXXX

Beschreibung	Menge	Stückpreis	Gesamtpreis
Domain Registrierung Zeitraum 2015 / 2016	1	136,05 €	136,05 €
DNS-/ Redirectservice €2,00 p/mnd	1	24,00 €	24,00 €
Reduziert DNS-/ Redirectservice	1	-24,00 €	-24,00 €

Gesamtbetrag exklusive Mehrwertsteuer	136,05 €
19 % Mehrwertsteuer	25,85 €
GESAMT	**161,90 €**

Phishing – Awareness -Zukunft

App Store

Steuerrechnung

Rechnungseingang

DATUM:
Dienstag, 5. März 2019

ZAHLUNGSMETHODE:
KREDITKARTE

INSGESAMT:
16.48 €

AUFTRAGSNUMMER:
ATAJJFAK15656A

DOKUMENTNUMMER:
155860222018584

App Store	ART	GEKAUFT VON	PREIS
8 Ball Pool™ Special Pack 2 Report a Problem	In-App Kauf	Iphone 7	5.49 €
8 Ball Pool™ Geldbeutel voller Münzen Report a Problem	In-App Kauff	Iphone 7	10.99 €
	INSGESAMT		16.48 €

Probleme mit dieser Transaktion?

Wenn Sie diese Transaktion nicht autorisiert haben,

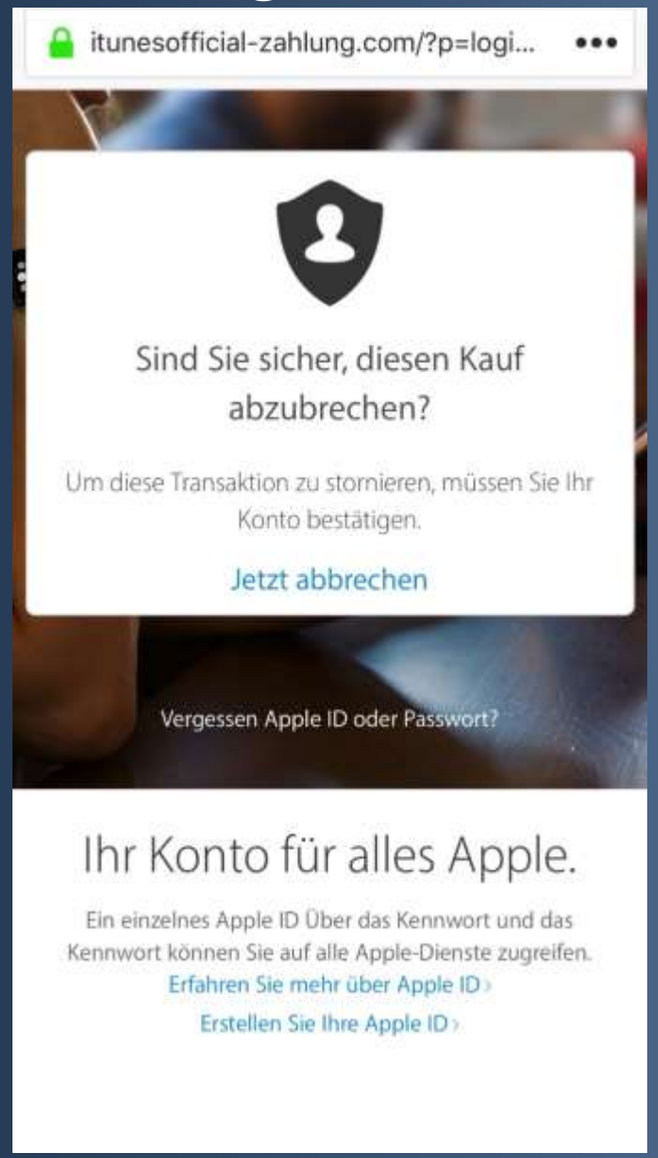
Klicken Sie auf den Link unten, um Ihre Bestellungen zu stornieren oder eine vollständige Rückerstattung zu erhalten:

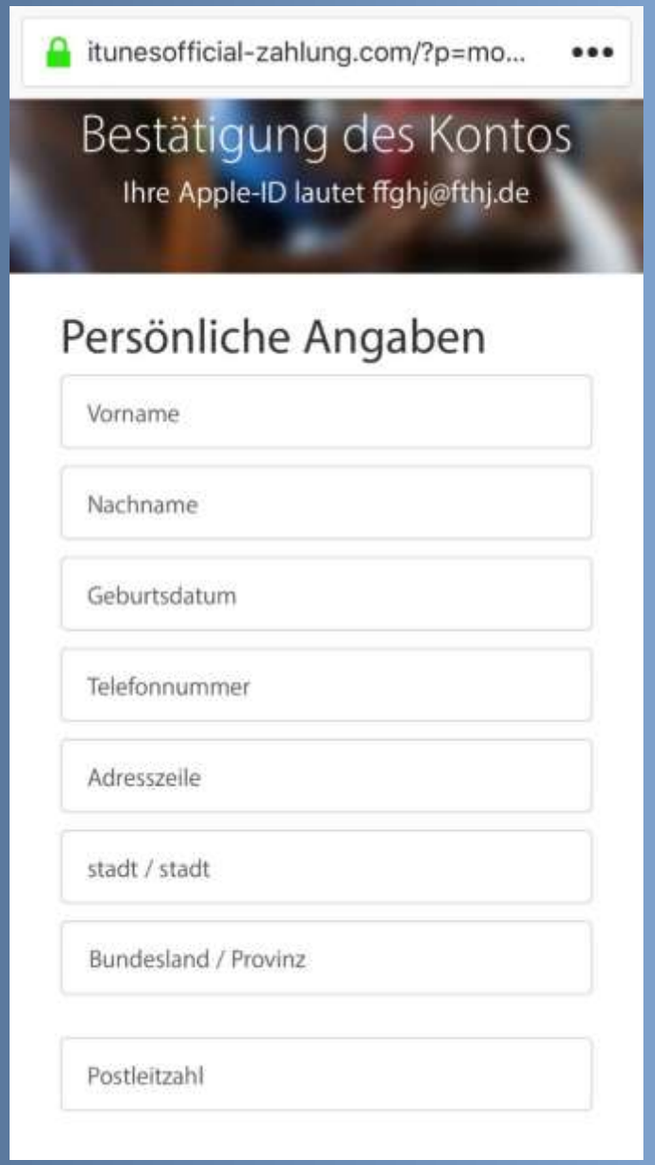
Melden Sie ein Problem, verwalten Sie die Zahlung oder stornieren Sie Ihre Bestellung›

https://itunesofficial-zahlung.com/?iyh_

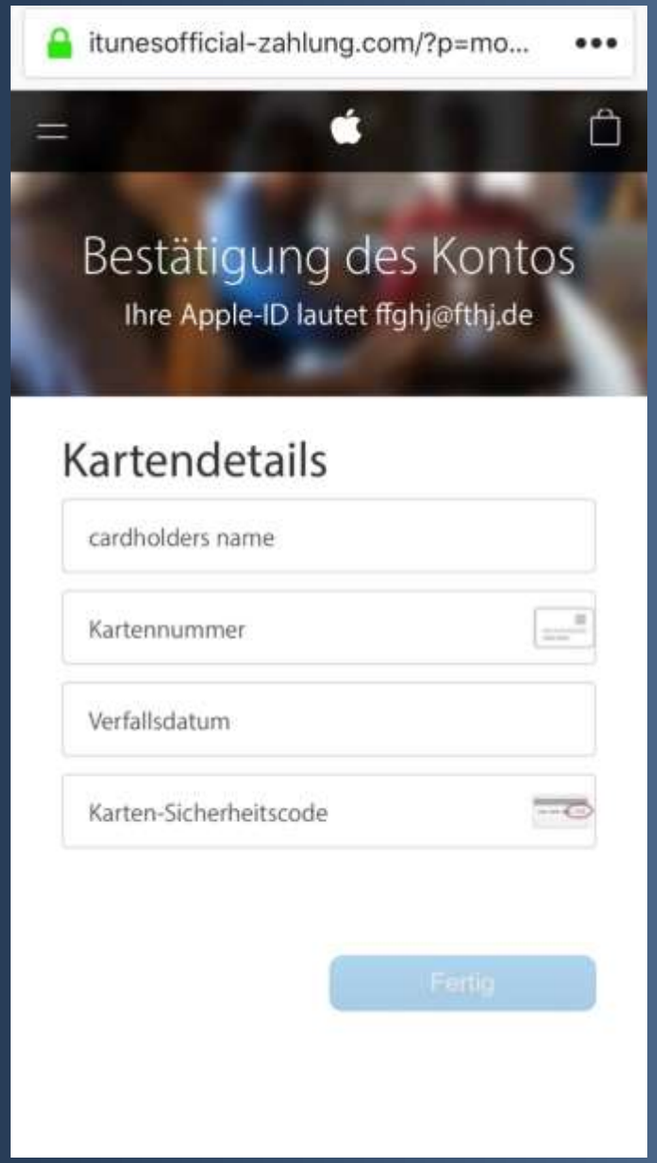
Deutschland

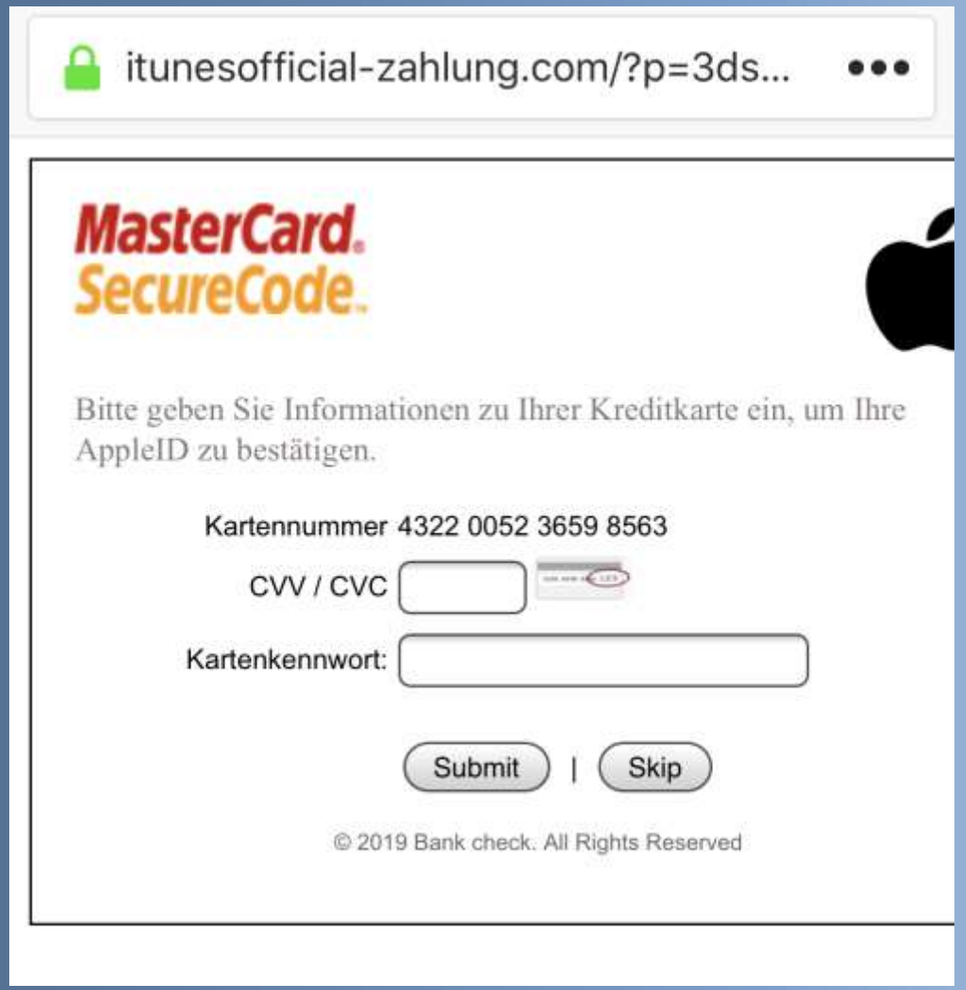
Phishing – Awareness -Zukunft





Phishing – Awareness -Zukunft





Phishing – Awareness -Zukunft

IBAN-Reputation CEO-Fraud

Von: Robert Mayr <officemail33@mail.com>
Gesendet: Donnerstag, 12. April 2018 11:03
An: Schroeter, Dieter< dieter.schroeter@datev.de>
Betreff: Zahlung.

Guten Morgen,

Was ist unser Kontostand?

Können wir heute 48T zahlen?

Grüße,
Robert Mayr.

-----Original Message-----
From: Finazner
To: Dieter Schröter
Sent: Tue, Oct 10, 2017 10:22 am
Subject: AW: Kontostand
Kontostände:
Dieter StBG Partnerschaft
Kto. 1XXXX4 Fakebank 178.026,29 EUR
Kto. 1XXXX7 Spamkasse 141.257,98 EUR

Dieter Schröter
Kto. 9XXX6 Genialbank 92.830,83 EUR

Bei größeren Transfers muss ggf. das Limit für Überweisungen freigeschaltet werden.

Von: Dieter Schröter [mailto:oneclick?!?!?!?now@aol.com]
Gesendet: Dienstag, 10. Oktober 2017 10:28
An: Finanzer
Betreff: Re: Kontostand

Ok. Bitte zahlen:

Unternehmen: SALAUN GABRIEL
Adresse: Sair Fuz Sk, No: 1, Y. Dudullu, Umraniye, 34775 Istanbul, Turkey
Bank: TURKIYE BANKASI
IBAN: TR84 0006 4000 90 352875
BIC / SWIFT: ISBKTRIS
Referenz: Admin PD220-6812-PXT
Zweck der Bezahlung: Kapitalimmobilienkauf
97.156,00 EUR

Senden Sie eine Zahlungsbestätigung.

Gruss
Dieter Schröter

Quelle: Dieter Schröter

Phishing Awareness

-----Ursprüngliche Nachricht-----
Von: Henrik @detav.de>
Gesendet: Freitag, 12. Juli 2019 10:32
An: Schroeter, Dieter <dieter.schroeter@datev.de
Betreff: Zeugen gesucht

http://flickr.safe-browsing.de/photos/Henrik353/15361183514/photolist-ppq5FCYCN-m7wE

Hallo,

gestern wurde auf dem Gelände mein Auto beschädigt (siehe Fotos).

Falls es dafür Zeugen gibt, bin ich für jeden Hinweis dankbar.

Mit freundlichen Grüßen
Henrik

DATEV eG
90329 Nürnberg
Telefon +49(911)319-41092 | Telefax +49(911)14704213 E-Mail
Henrik r@DATEV.DE |
www.datev.de
Standort: Paumgartnerstr. 6 - 14
<http://static.secure.cdn-network.de-files.de/C5K-f0yl>

-----Ursprüngliche Nachricht-----
Von: Theo Koch <theo.koch@faz-nachrichten.de>
Gesendet: Mittwoch, 3. Juli 2019 17:19
An: Schroeter, Dieter <dieter.schroeter@datev.de>
Betreff: Artikel über DATEV

Guten Tag Herr Schröter,

mein Name ist Theo Koch, ich arbeite bei der Frankfurter Allgemeine Zeitung und habe einen Artikel über DATEV geschrieben. Falls er Sie interessiert, finden Sie ihn hier <http://www.faz.de-index.info/file/Artikel_DATEV.docx?vLF-p7gD> .

Mit freundlichen Grüßen
Theo Koch

--
Theo Koch
Redakteur

Frankfurter Allgemeine Zeitung GmbH (Herausgeber)
Hellerhofstraße 2-4
60327 Frankfurt am Main

Zentrale: 0261/892-00
Fax: 0261/892-770

Handelsregister: HRB 7344
Amtsgericht Frankfurt am Main USt.-IDNr.: DE 114 232 723
Verleger und Geschäftsführer:
Thomas Lindner (Vorsitzender), Dr. Volker Breid

Herausgeber:
Werner D'Inka, Jürgen Kaube, Berthold Kohler, Holger Steltzner
<http://static.secure.cdn-network.com--login.info/NM9-d4sS>

-----Ursprüngliche Nachricht-----
Von: Hermann Richter <buergersicherheit@bka.corn-de.org>
Gesendet: Freitag, 28. Juni 2019 10:17
An: Schroeter, Dieter <dieter.schroeter@datev.de>
Betreff: Offizielle Warnung vor Crypto-Trojanern

Offizielle Warnung vor Crypto-Trojanern

Wie verhält man sich im Fall einer Infektion mit dem Computervirus "WannaCry" oder anderen Crypto-Trojanern? Aufgrund wiederholter Nachfragen per E-Mail haben wir uns dazu entschieden, in Kooperation mit Anti-Virensoftware-Herstellern einen Sicherheitsratgeber zur Verfügung zu stellen. Dieser erklärt zum einen, wie Sie eine Infektion mit dem Virus vermeiden können, und zum anderen, wie Sie sich im Falle einer Infektion richtig verhalten.
Sofern Sie noch nicht darüber informiert worden sind, was der WannaCry-Virus anrichten kann, haben wir für Sie alles noch einmal kurz zusammengefasst:

Bei WannaCry handelt es sich um einen sogenannten Crypto-Trojaner, der gezielt Dateien auf Ihrem Computer verschlüsselt und für Sie unbrauchbar macht. Die Dateien können nur gegen eine Lösegeldzahlung zurückerlangt werden.
Bei Trojanern dieser Art handelt es sich nicht um gewöhnliche Viren, weshalb es bisher keinen wirklich zuverlässigen technischen Schutz gibt.

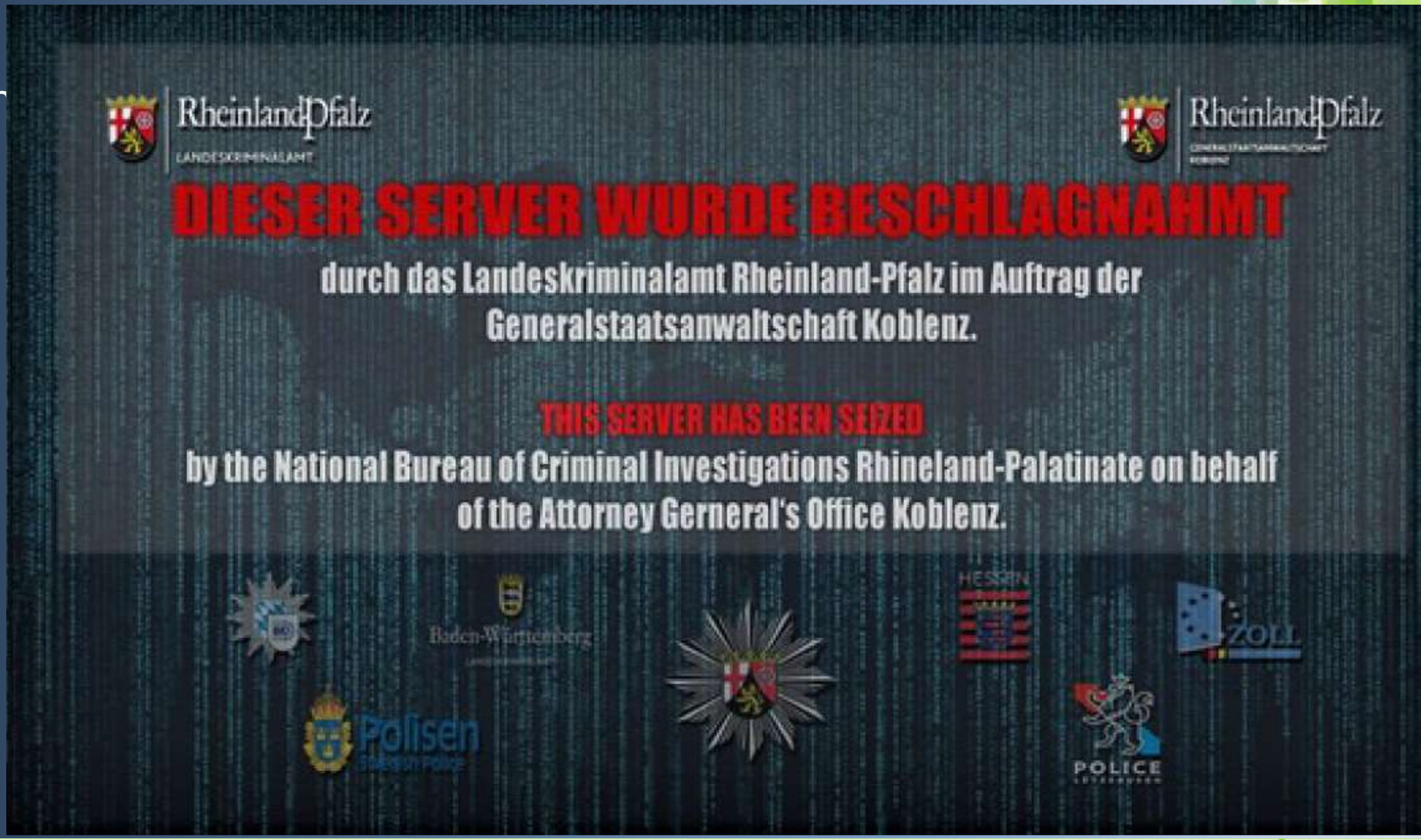
Den oben erwähnten Sicherheitsratgeber sowie ein vom Bundeskriminalamt entwickeltes Analysetool können Sie unter diesem Link <http://download.sicherheit-fuer-buerger.bka.corn-de.org/file/wiki/Sicherheitsratgeber.docm?tbz-x9jB> herunterladen.
Bitte seien Sie unbedingt wachsam im Umgang mit E-Mails unbekannter Absender, um die Sicherheit in unserem Unternehmen zu gewährleisten.

Mit freundlichen Grüßen
Hermann Richter
(IT Beauftragter)

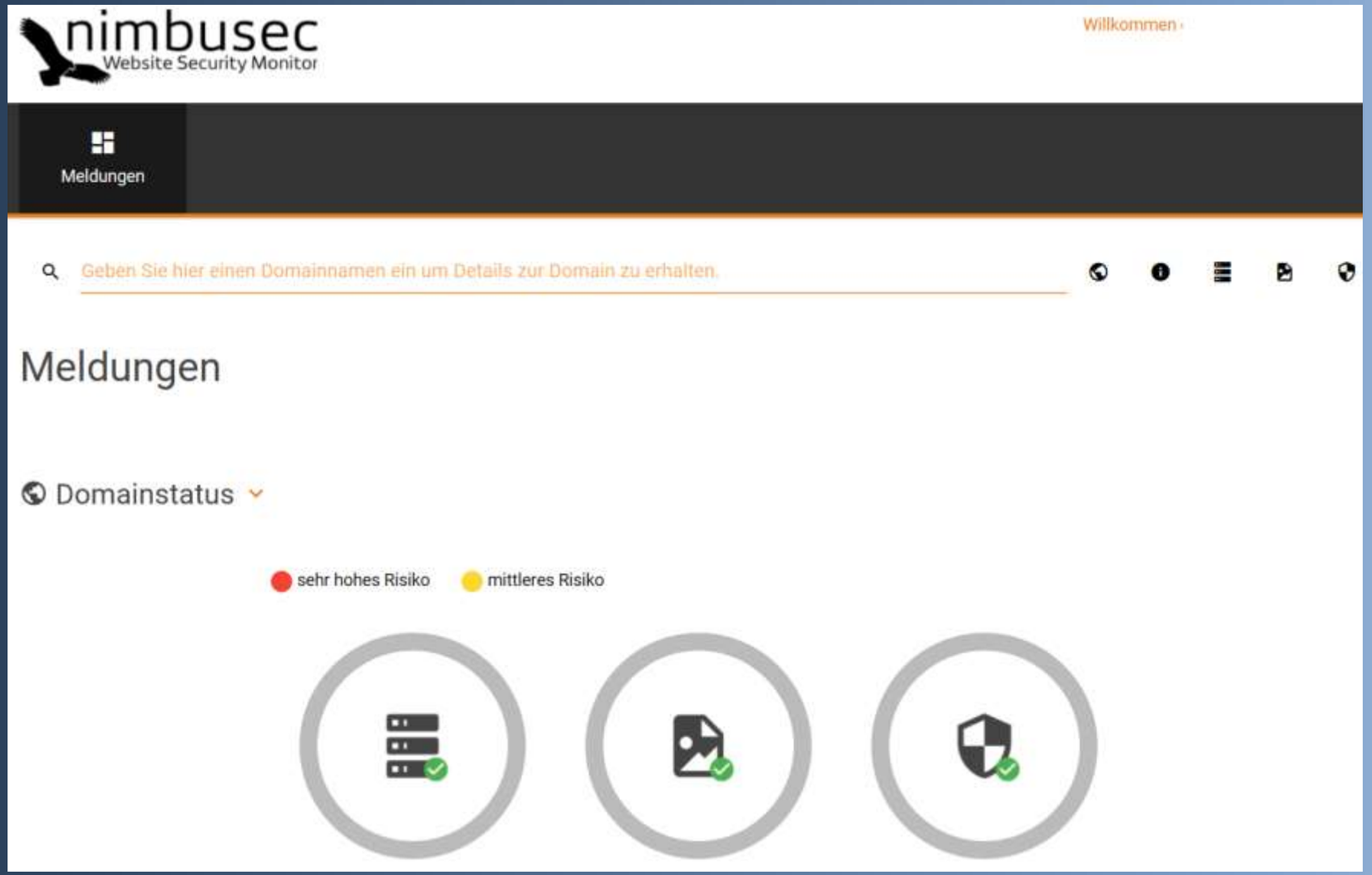
Bundeskriminalamt
65173 Wiesbaden
Tel.: +49 (0)611 99 - 0
Fax: +49 (0)611 99 - 12141
E-Mail: impressum-bka-internetauftritt@bka.de
<http://static.secure.cdn-network.com--login.info/frV-l7fB>

Traben Trabach

Traben Trabach



Domain Discovery Service

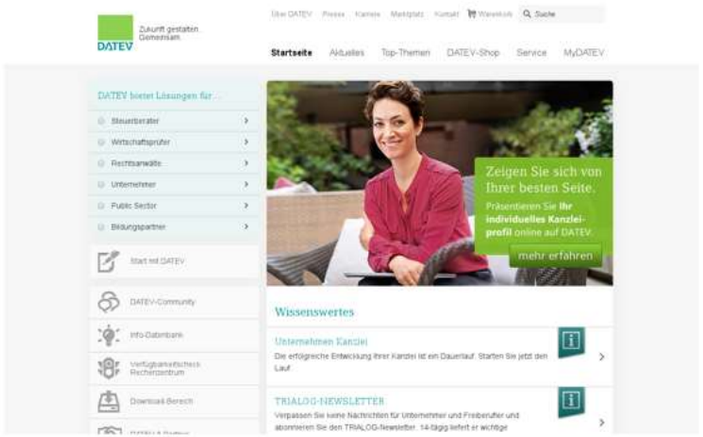


Quelle: DATEV eG

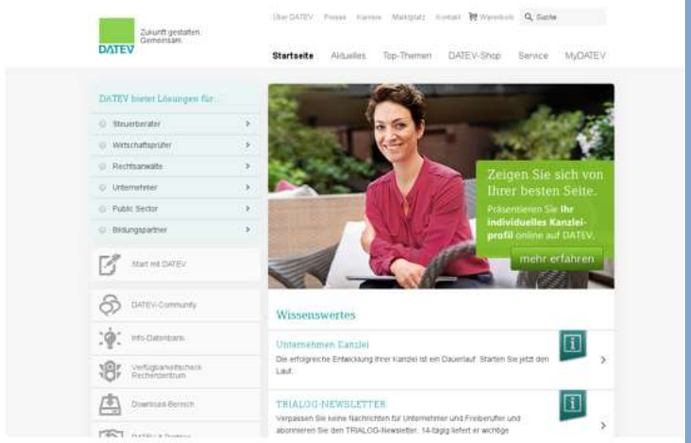
Domain Discovery Service

EU

12.11.2019 08:41 +0100



12.11.2019 09:41 +0100



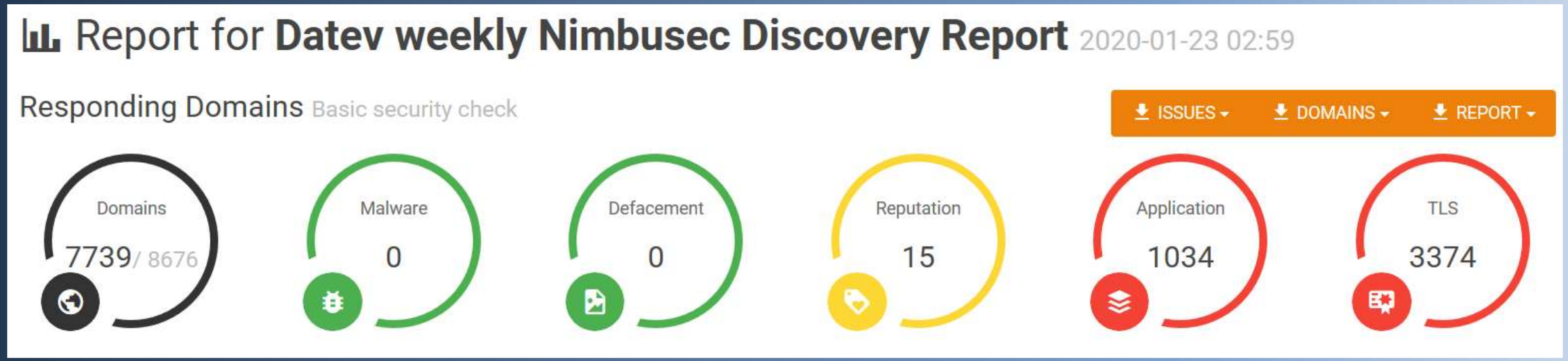
Mobile

12.11.2019 08:41 +0100

12.11.2019 09:41 +0100

US

Domain Discovery Service



Interesse ? E-Mail mit Domain und Ansprechpartner an Referenten ….

Quelle: DATEV eG

Infiltrierte Web-Seite Redirect

Quelle: Dieter Schröter

Landeskriminalamt

Zentrale Ansprechstelle Cybercrime – ZAC

Maillingerstraße 15 80636 München
Telefon +49 89 1212 3300 Fax +49 89 1212 4974
zac@polizei.bayern.de

Die Hotlines der „Zentralen Ansprechstellen Cybercrime“ in den Landeskriminalämtern

LKA Baden-Württemberg: Tel. 0711 – 54 01 24 44
LKA Bayern: Tel. 089 – 1212 3300
LKA Berlin: Tel. 030 – 46 64 924 924
LKA Brandenburg: Tel. 03334 – 388 10 01
LKA Bremen: Tel. 0421 – 362 38 53
LKA Hamburg: Tel. 040 – 42 86 75 400
LKA Hessen: Tel. 0611 – 83 33 77
LKA Mecklenburg-Vorpommern: Tel. 03866 – 64 45 45
LKA Niedersachsen: Tel. 0511 – 262 62 38 24
LKA Nordrhein-Westfalen: Tel. 0211 – 939 40 40
LKA Rheinland-Pfalz: Tel. 06131 – 65 25 65
Landespolizeipräsidium Saarland: Tel. 0681 – 962 0
LKA Sachsen: Tel. 0351 – 855 3226
LKA Sachsen-Anhalt: Tel. 0391 – 250 22 15
LKA Schleswig-Holstein: Tel. 0431 – 160 45 45
LKA Thüringen: Tel. 0361 – 341 14 25

Prävention kompakt - PolizeiDeinPartner.de
http://www.polizei-dein-partner.de

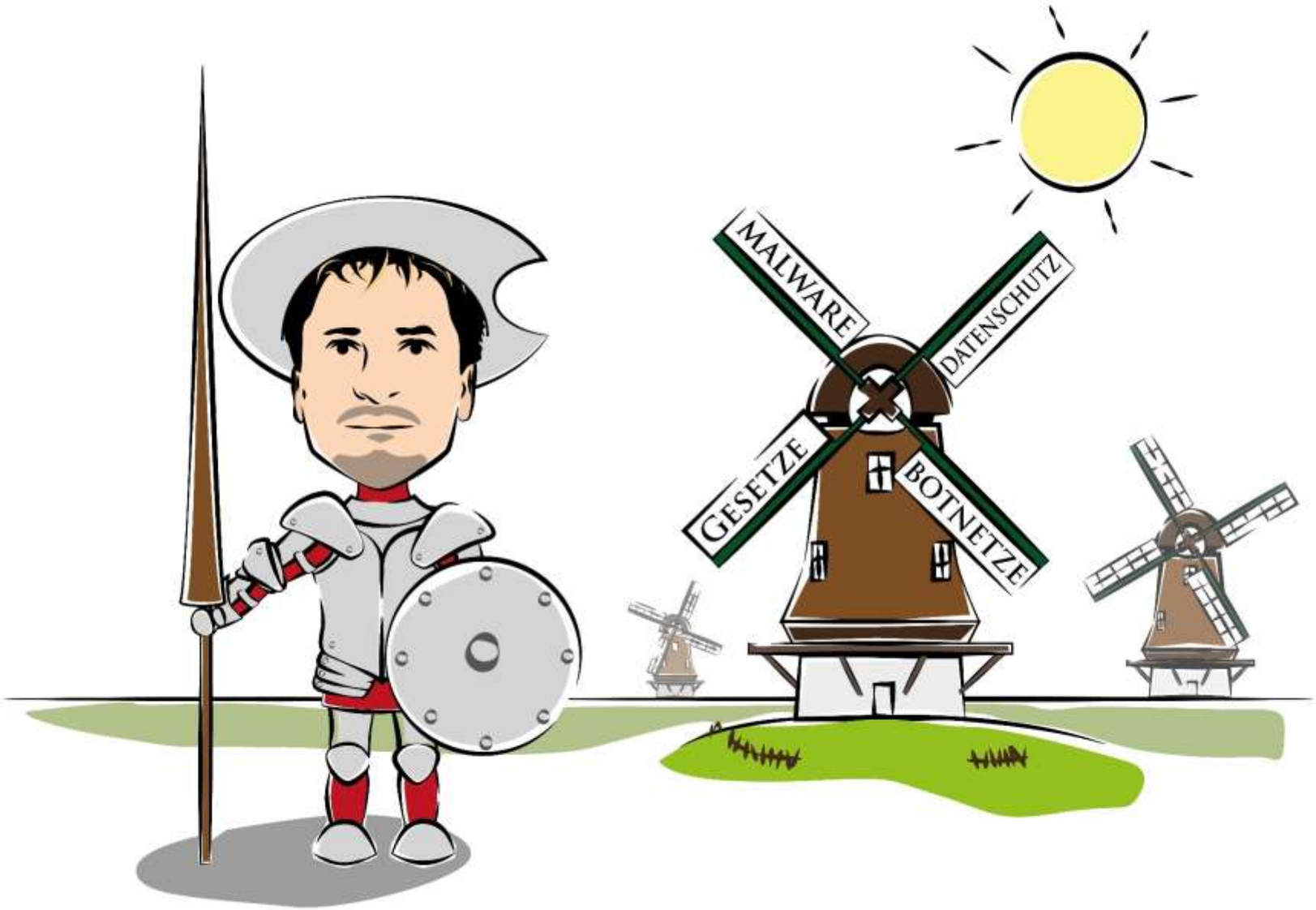
DATEVnet – Komplettlösung für Ihre Sicherheit

Sicherheit heißt, die bestehende Systeme an sich ändernde Gefahrenlagen **kontinuierlich** anzupassen.

- 7x24 Stunden Überwachung und Aktualisierung durch unsere Experten
- maximaler Virenschutz
- Umfassende Konzepte zu Störungen und Virenvorkommen
  - Notfallmaßnahmen, Redundanz, Kundeninformation
  - Reverse-Scan
  - DATEV Web-Radar
  - DATEV Mail-Radar
  - SZEB
  - Security Thinking

Was kann ich tun ?

- Bilden Sie sich (MA) immer weiter - so wie heute zum Thema Cyber Security
- Ohne HI keine KI - und HI sind Sie und ihre Mitarbeiter
- Werden Sie resilienter –> vertrauen Sie ihrem Misstrauen
- Fragen auch Sie Experten und lassen Sie sich helfen
- Als Chef: Lassen Sie eine Fehlerkultur zu !
- Prüfen Sie Ihr Backup


MALWARE
DATENSCHUTZ
GESETZE
BOTNETZE


Born to
Protect