

MFG

Nun, da sich der Vorhang der Nacht von der Bühne hebt
Kann das Spiel beginnen
Das uns vom Drama einer Kultur berichtet

Dieser Talk

- Ich mache IT für KMUs seit 2017
 - Betreibe eigene E-Mail Server seit 2009
- Schrödingers Fortsetzung von «What the BEC?»
- Beginnt mit einer E-Mail
- Endet mit vielen Fragen

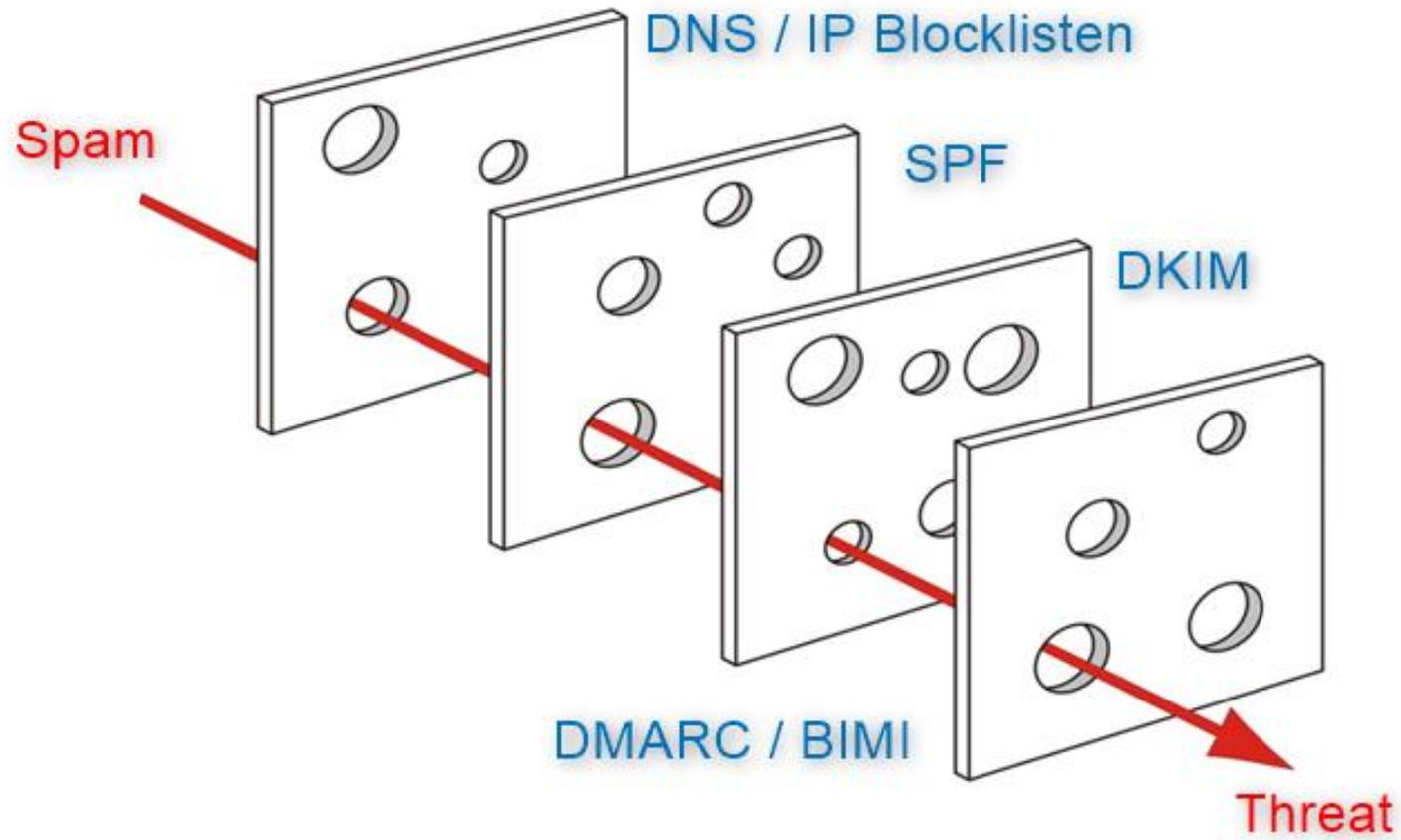
BEC?

- Erfolgreicher Phishingversuch
- Meist im Businessumfeld
- Macht keinen Spass, weitere Angriffe kosten viel Geld.
- Erzwingt (meist) Kundenbenachrichtigung nach DSGVO

DNS, SPF, DKIM

- SMTP wurde 1981 in RFC 788 das erste mal spezifiziert
- SPF wurde 2006 experimentell spezifiziert
- DKIM wurde 2011 spezifiziert
- DMARC 2015

DNS, SPF, DKIM



DNS, SPF, DKIM

- Zwingend für die Mailübertragung sind: TCP/IP & DNS und SMTP
- Alles weitere sind Pflasterli
- Trotzdem kommt Spam noch durch

TCP / IP / DNS	Grundlagen
SMTP	Grundlagen
SSL / TLS	Sicherheit
DNSBL	Externer Ruf
Graylisting	Verzögerung
SPF	Selbstdeklarativ
DKIM	Absendersignatur
DMARC	Selbstdeklarativ
Spam-Filter	Mustererkennung
Antivirus	Signaturerkennung

Kurzer Exkurs

- Spamversand ist heute also schwierig
- Umso wichtiger ist es, Accounts zu kompromittieren
- Damit können Angreifer die ganzen technischen Massnahmen für sich nutzen

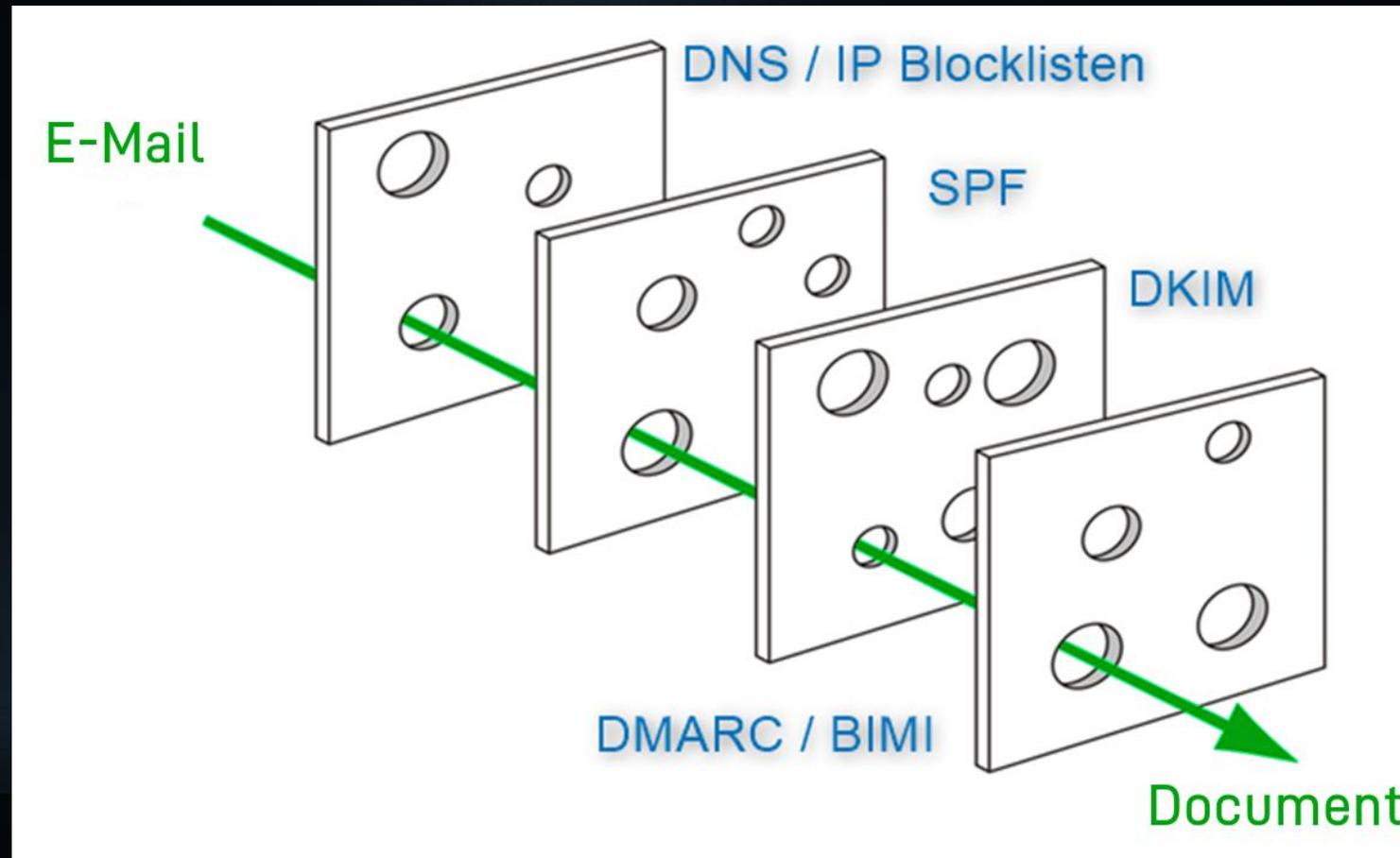
TCP / IP / DNS	Grundlagen
SMTP	Grundlagen
SSL / TLS	Sicherheit
DNSBL	Externer Ruf
Graylisting	Verzögerung
SPF	Selbstdeklarativ
DKIM	Absendersignatur
DMARC	Selbstdeklarativ
Spam-Filter	Mustererkennung
Antivirus	Signaturerkennung

Kurzer Exkurs

- DNSBL nützen sowieso kaum noch, weil kaum jemand Microsoft als ganzes blockieren kann oder will, weil so viele den Dienst nutzen.
- Der Vorteil der Dezentralisierung ging verloren
- Aber in der Cloud ist alles besser

TCP / IP / DNS	Grundlagen
SMTP	Grundlagen
SSL / TLS	Sicherheit
DNSBL	Externer Ruf
Graylisting	Verzögerung
SPF	Selbstdeklarativ
DKIM	Absendersignatur
DMARC	Selbstdeklarativ
Spam-Filter	Mustererkennung
Antivirus	Signaturerkennung

DNS, SPF, DKIM



DHL Express / Sendungsreport März 2025

 (DHL CH) <[redacted]@dhl.com>
An [redacted]

↩ Antworten

↩ Allen antworten

→ Weiterleiten



Mo. 07.04.2025 10:19

 [redacted] Diagnostics_MAR 25.xlsm .xlsm-Datei ▾

Guten Morgen [redacted]

im Anhang sende ich Ihnen die Sendungsübersicht für den Monat März 2025.

Achtung – aufgrund erweiterter Sicherheitsvorkehrungen im Bereich Datenschutz wird der Report verschlüsselt an Sie versendet. Das Passwort zum Öffnen des Files lautet [redacted]. Danach erhalten Sie wie üblich Zugriff und Einsicht.

Wünsche einen guten Start in die Woche.

Freundliche Grüsse

[redacted]
Executive

DHL Express (Schweiz) AG

[redacted]

Telefon: +41 79 [redacted]
[redacted]@dhl.com

[Ihre DHL Express Kontakte](#)

[Preis Anfrage für schwere internationale Sendungen ab 50 Kg bis 3'000 Kg](#)

https://express-resource.dhl.com/rs/***-***-***/images/ch-factsheet--contact-sheet-*****-*-german-download.pdf

https://i.emlfiles4.com/cmpdoc/3/5/8/7/files/*****_**_dhl_editierbares-gsrt-formular_****.de.pdf

DHL, XLS , ihr könnt mich mal

Person als Absender

Excel mit Makros im Anhang

Verschlüsselung mit Passwort

Telefonnummer: Handynummer

Kontaktlink: dhl.com

Preisanfrage: emlfiles4.com

DHL Express / Sendungsreport März 2025

(DHL CH) <@dhl.com>

Mo. 07.04.2025 10:19

Antworten | Allen antworten | Weiterleiten | ...

Diagnosics_MAR 25.xlsm .xlsm-Datei

Guten Morgen

im Anhang sende ich Ihnen die Sendungsübersicht für den Monat März 2025.
Achtung – aufgrund erweiterter Sicherheitsvorkehrungen im Bereich Datenschutz wird der Report verschlüsselt an Sie versendet. Das Passwort zum Öffnen des Files lautet . Danach erhalten Sie wie üblich Zugriff und Einsicht.

Wünsche einen guten Start in die Woche.

Freundliche Grüße

Executive

DHL Express (Schweiz) AG

Telefon: +41 79 @dhl.com

[Ihre DHL Express Kontakte](#)

Preisanfrage für schwere internationale Sendungen ab 50 Kg bis 3'000 Kg

https://express-resource.dhl.com/rs/903-EZK-832/images/ch-factsheet--contact-sheet-****-*-german-download.pdf

https://i.emlfiles4.com/cmpdoc/3/5/8/7/files/*****_dhl_editierbares-gsrt-formular_v.6.1.de.pdf

Echt oder Fake?

ECHT

DHL, XLS , ihr könnt mich mal

Person als Absender

Vertrauen schaffen? Manueller Versand?

Excel mit Makros im Anhang

Warum Makros?

Verschlüsselung mit Passwort

Obfuscation (Antivirus / Anti-Spam)

Telefonnummer: Handynummer

Warum keine Haupt oder Direktnummer?

Kontaktlink: dhl.com

Scheint legitim

Preisanfrage: emlfiles4.com

Was ist das für eine URL?

Anhang öffnen oder nicht?

Zwischenstand

- Mindestens 7 technische Hürden mussten überwunden werden
- 2-3 Vertrauensmassnahmen: Versand durch Betreuer, Mobil-Nr direkt & Kontaktinfos von DHL.com herunterladbar.
- Nun kann die Datei geöffnet werden!

DHL, XLS, ihr könnt mich mal

Automatisches Speichern   

Pulse-Diagnostics_MAR 25.xlsm - Geschützte An... • Auf "diesem PC" gespeichert

Suchen

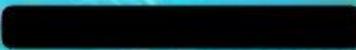
Datei Start Einfügen Seitenlayout Formeln Daten Überprüfen Ansicht Automatisieren Hilfe Acrobat

GESCHÜTZTE ANSICHT Vorsicht — Dateien aus dem Internet können Viren enthalten. Wenn Sie die Datei nicht bearbeiten müssen, ist es sicherer, die geschützte Ansicht beizubehalten.

Bearbeitung aktivieren

P34   


DHL EXPRESS PERFORMANCE MANAGEMENT

Report created for 

This report contains confidential data. It is provided for information purposes only and should not be used for any other purposes.

DHL reserves all rights to rectification of data.



World Map

Trade Lane Summary

Trend Analysis

Deep Dive

Detail Data

Continuous Improvement

Quick Reference

Contact and Support



Customer Name:

Data preparation completed!

Reporting Months: [Mar '25]

Week Range: [2025 Week 10] to [2025 Week 14]

Please Click the "Enable Editing" on the top bar if you are opening this report in read-only format:

 Protected View This file originated as an e-mail attachment and might be unsafe. Click for more details. [Enable Editing](#)

Please also click the "Enable Content" on the top bar in order to use this report the way it was intended:

 Security Warning Macros have been disabled. [Enable Content](#)

DHL, XLS , ihr könnt mich mal

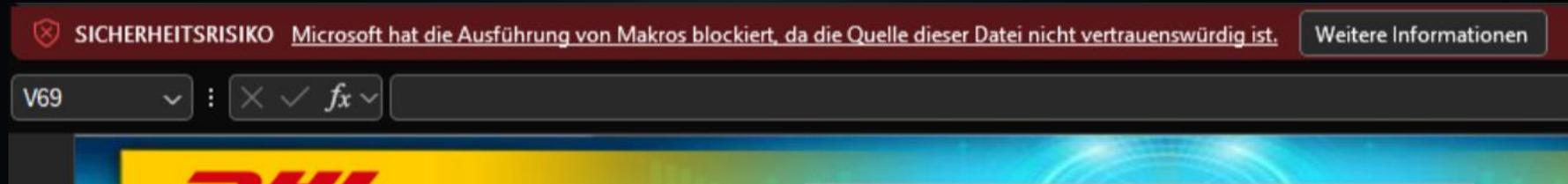
Mark of the Web: Makros aus!

Bearbeitungsschutz:
Office

«Inhalt aktivieren»:
Makrosicherheit

The screenshot shows a Microsoft Excel spreadsheet titled "Pulse-Diagnostics_MAR 25.xlsm". The interface is in German. A red security warning banner at the top states: "SICHERHEITSRISIKO Microsoft hat die Ausführung von Makros blockiert, da die Quelle dieser Datei nicht vertrauenswürdig ist." Below this, a report interface is visible with a header "Report created for" followed by a redacted name. A navigation bar contains tabs: "Trade Lane Summary", "Trend Analysis", "Deep Dive", "Detail Data", "Continuous Improvement", and "Quick Reference". Below the tabs, there is a field for "Customer Name:" followed by a redacted name. The main content area displays "Data preparation completed!" and "Reporting Months: [Mar '25]" and "Week Range: [2025 Week 10] to [2025 Week 14]". At the bottom, there are two security warning bars. The first bar says "Protected View This file originated as an e-mail attachment and might be unsafe. Click for more details." and has an "Enable Editing" button. The second bar says "Security Warning Macros have been disabled." and has an "Enable Content" button.

VBS, MotW, ohjemine



«Gibt es einen Trick, wie ich das Sicherheitsrisiko auf mich nehmen kann um einen Report von DHL zu lesen?»»

Vorgehen

1. Datei öffnen
2. Bearbeiten aktivieren
3. Inhalt kann nicht aktiviert werden => Datei schliessen
4. Mark of the Web entfernen (Rechtsklick > Eigenschaften > Vertrauen)
5. Datei öffnen
6. Bearbeiten aktivieren
7. Inhalt aktivieren

Zwischenstand

- Mindestens **10** technische Hürden mussten überwunden werden
- 2-3 Vertrauensmassnahmen: Versand durch Betreuer, Mobil-Nr direkt & Kontaktinfos von DHL.com herunterladbar.
- Nun ist die Datei offen.

Na und?

- Benutzer lernen die Sicherheitsmechanismen zu umgehen
- Wir wiederholen nun das Training für das Öffnen von potentiell schädlichen Excel-Dateien mit Makros jetzt einmal im Monat

Wie oft macht ihr
Anti-Phishing-Trainings?

MFG, CyberCrime

Wie aktuell sind die
Arbeitsgeräte eurer HR und
Buchhaltungsabteilung?

MFG, CyberCrime

Ja aber...

- Aber! Dafür mussten 10 technische Hürden genommen werden!
- Und wir haben ja bestimmt eine super Fehlerkultur aufgebaut!
- Und nutzen phishingresistente Multifaktor-Methoden

CYBER

CYBER

CYBER

Cyberstudie 2024

2021 – 2024: 4% der befragten KMU hatten: «Schwerwiegende Cyberattacke»

73 % der Betroffenen sagen: «erheblicher finanzieller Schaden»

40% Der Unternehmen haben keinen Notfallplan und keine BCI

IT-Dienstleistende empfehlen Schweizer KMU, das Thema Sicherheit ernster zu nehmen (43 %) und ihr Personal zu schulen (29 %).

Die Befragten sind mehrheitlich der Meinung, eher gut bis sehr gut Bescheid zu wissen, wie sie sich vor Cyberangriffen schützen können.

CYBER

CYBER

CYBER

“Die Befragten sind mehrheitlich der Meinung, eher gut bis sehr gut Bescheid zu wissen, wie sie sich vor Cyberangriffen schützen können.“

Zwischenstand

- Mindestens **10** technische Hürden mussten überwunden werden
- 2-3 Vertrauensmassnahmen: Versand durch Betreuer, Mobil-Nr direkt & Kontaktinfos von DHL.com herunterladbar.
- Unsere Benutzer können nun Zielsicher MotW und Makroschutz ausschalten.

BEC

Die Welt liegt uns zu Füßen
denn wir stehen drauf
Wir gehen drauf
für ein Leben voller Schall und Rauch

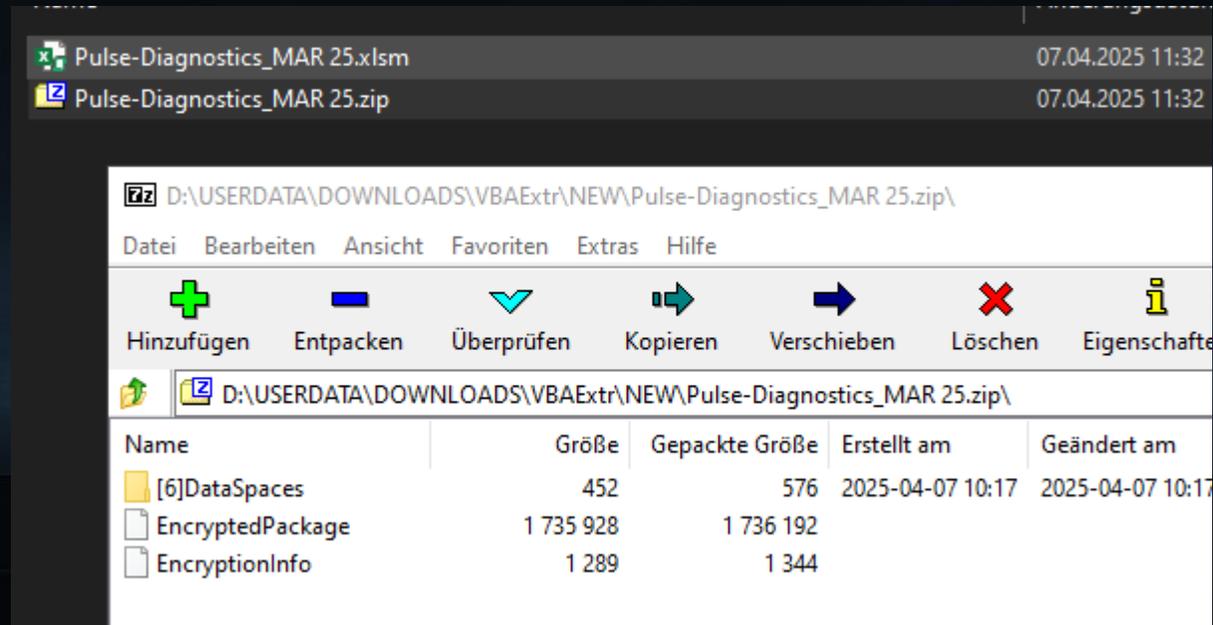
Zwischenstand

- Passkeys & FIDO2 wären die Lösung
- Einrichtung und Onboarding ist selbst im besten Fall... zäh.
 - (Und der Ablauf ändert sich auch konstant...)

Wofür das
alles?

ZIP, DPB und HdX

- Exceldateien sind auch nur ZIP-Archive
- Umbenennen & Extrahieren...

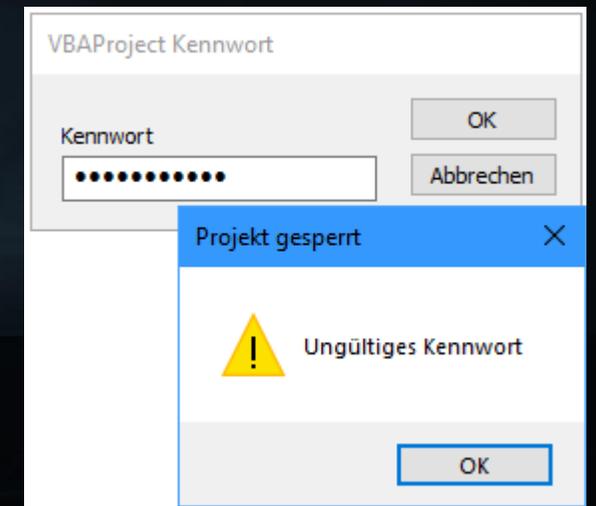


ZIP, DPB und HxD

- Lernen dass Excel mittlerweile echt mit AES256 verschlüsselt ...
- Zum Glück wissen wir ja das Passwort, es steht im Mail:

Achtung – aufgrund erweiterter Sicherheitsvorkehrungen im Bereich Datenschutz wird der Report verschlüsselt an Sie versendet. Das Passwort zum Öffnen des Files lautet [REDACTED] Danach erhalten Sie wie üblich Zugriff und Einsicht.

- Aber der Zugriff auf die VB Lösung ist auch passwortgeschützt... und sogar durch ein anderes!



ZIP, DPB und HxD

- Wäre ja schade wenn dem VBA Projekt etwas zustossen würde...



D:) > USERDATA > DOWNLOADS > VBAExtr > extracted > xl

Name	Änderungsdatum	Typ	Größe
terne	07.04.2025 11:57	Dateiordner	
worksheets	07.04.2025 11:57	Dateiordner	
calcChain.xml		XML-Datei	19 KB
sharedStrings.xml		XML-Datei	116 KB
styles.xml		XML-Datei	50 KB
vbaProject.bin	07.04.2025 12:16	BIN-Datei	700 KB
workbook.xml		XML-Datei	8 KB

HxD - [D:\USERDATA\DOWNLOADS\VBAExtr\extracted\xl\vbaProject.bin]

Datei Bearbeiten Suchen Ansicht Analyse Extras Fenster Hilfe

16 Windows (ANSI) hex

vbaProject.bin

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Dekodierter Text
00000000	B0	CF	11	E0	A1	B1	1A	E1	00	00	00	00	00	00	00	00	BI.à;±.á.....
00000010	00	00	00	00	00	00	00	00	3E	00	03	00	FE	FF	09	00>...pÿ..
00000020	06	00	00	00	00	00	00	00	00	00	00	00	0B	00	00	00
00000030	01	00	00	00	00	00	00	00	00	10	00	00	02	00	00	00
00000040	05	00	00	00	FE	FF	FF	FF	00	00	00	00	00	00	00	00pÿÿÿ.....
00000050	51	00	00	00	E1	00	00	00	6A	01	00	00	00	02	00	00	Q...á...j.....

ZIP, DBP und HxD

- Einmal den Begriff DPB suchen...
- und den DPB mit DPx ersetzen

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Dekodierter Text	
000AE920	0A	4E	61	6D	65	3D	22	56	42	41	50	72	6F	6A	65	63	.Name="VBAProjec	
000AE930	74	22	0D	0A	48	65	6C	70	43	6F	6E	74	65	78	74	49	t"..HelpContextI	
000AE940	44	3D	22	30	22	0D	0A	56	65	72	73	69	6F	6E	43	6F	D="0"..VersionCo	
000AE950	6D	70	61	74	69	6E	62	6C	65	33	32	3D	22	33	39	33	32	
000AE960	32	32	30	30	30	22	0D	0A	43	4D	47	3D	22	46	39	46		
000AE970	41	43	34	31	32	41	33	35	39	41	33	35	39	41	36	35	45	41
000AE980	37	43	44	22	0D	0A	44	50	78	3D	22	22	0D	0A	47	43	65	E"..DPx=""..GC
000AE990	45	46	33	31	30	31	30	30	30	31	3D	7B	33	38	33	32	44	= "797BD526D626D6
000AE9A0	31	31	30	45	35	41	33	35	39	41	33	35	39	41	36	35	45	26"....[Host Ext
000AE9B0	42	46	33	45	30	31	30	30	30	30	31	3D	7B	33	38	33	32	ender Info]..&H0
000AE9C0	42	45	43	44	30	31	30	30	30	30	31	3D	7B	33	38	33	32	0000001={3832D64
000AE9D0	39	41	44	39	37	21	30	30	30	30	31	3D	7B	33	38	33	32	0-CF90-11CF-8E43
000AE9E0	39	34	45	37	39	31	30	30	30	30	31	3D	7B	33	38	33	32	-00A0C911005A};V
000AE9F0	0A	5B	48	6F	73	77	00	00	00	00	00	00	00	00	00	00	00	
000AFA00	49	6E	66	6E	5D	00	00	00	00	00	00	00	00	00	00	00	00	

vbaProject.bin

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Dekodierter Text	
000E8E80	44	3D	22	30	22	0D	0A	56	65	72	73	69	6F	6E				
000E8E90	6D	70	61	74	69	6E	62	6C	65	33	32	3D	22	33	39	33	32	
000E8EA0	32	32	30	30	30	22	0D	0A	43	4D	47	3D	22	46	39	46		
000E8EB0	42	35	35	41	33	35	39	41	33	35	39	41	36	35	45	41		
000E8EC0	36	35	45	22	0D	0A	44	50	78	3D	22	22	0D	0A	47	43		
000E8ED0	3D	22	37	39	37	42	44	35	32	36	44	36	32	36	44	36		
000E8EE0	32	36	22	0D	0A	0D	0A	5B	48	6F	73	74	20	45	78	74		
000E8EF0	65	6E	64	65	72	20	49	6E	66	6F	5D	0D	0A	26	48	30		
000E8F00	30	30	30	30	30	30	31	3D	7B	33	38	33	32	44	36	34		
000E8F10	30	2D	43	46	39	30	2D	31	31	43	46	2D	38	45	34	33		
000E8F20	2D	30	30	41	30	43	39	31	31	30	30	35	41	7D	3B	56		

Microsoft Visual Basic for Applications

Unerwarteter Fehler (40230)

Allgemein Schutz

Projekt sperren

Projekt für die Anzeige sperren

Wofür das
alles?

Wie kommt
das?

Gäbe es nicht bessere Methoden?

The screenshot displays the DHL Express MyDHL+ interface. At the top, the DHL logo and 'DHL Express' are on the left, and navigation links for 'Hilfe und Support', 'Einen DHL Standort finden', and language options (English, Deutsch, Français, Italiano) are on the right. Below this is a secondary navigation bar with 'Home', 'Versenden', 'Verfolgen', and 'Verwalten' (with a notification badge '0'). On the right of this bar are links for 'Rechnungen verwalten', 'Meine Einstellungen', and 'Mein Profil'.

The main content area starts with a welcome message: 'Willkommen zu MyDHL+'. Below it is a blue notification box titled 'Änderung des Anmeldeverfahren' (Change of login procedure), stating that MyDHL+ is updating its login process for security and comfort, with a link to 'Mehr erfahren'.

The central part of the page is a shipping form with tabs: 'Neue Sendung' (highlighted), 'Aus Favoriten', 'Aus Historie', 'Abholung buchen', and 'Preis anfragen'. The form is divided into two sections, A and B, connected by a vertical dotted line. Section A is for the origin, with 'Land/Territorium' set to 'Switzerland' and 'Von' (Street, City, ZIP, Country) as a text input. Section B is for the destination, with 'Land/Territorium' as a dropdown and 'An' (Street, City, ZIP, Country) as a text input. A yellow 'Wechseln' button is between the sections. A green 'Weiter' button is at the bottom right of the form.

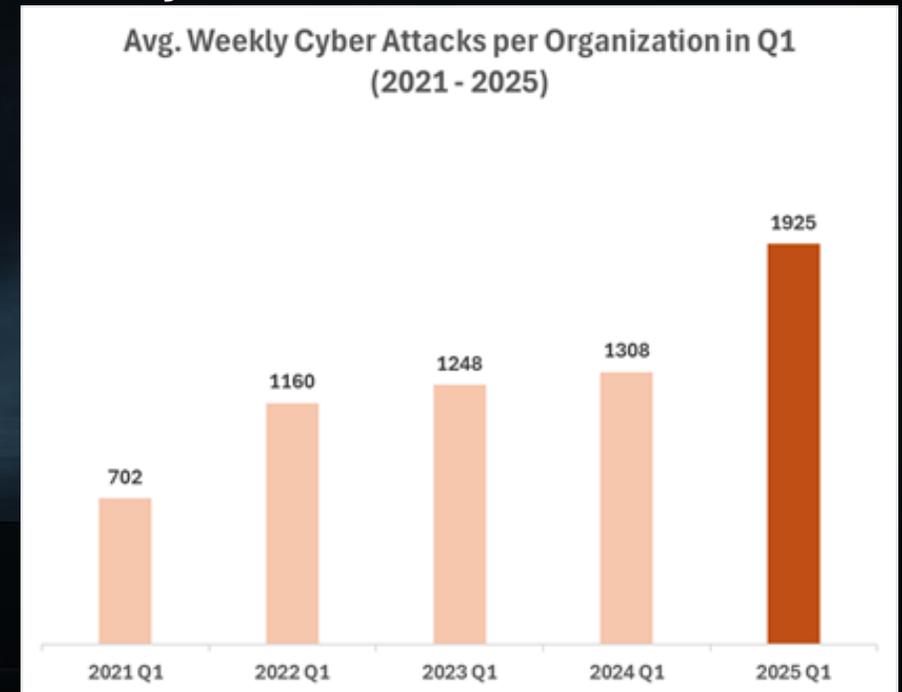
On the right side, there are two panels. The top one is 'Meine Sendungen' (My Shipments), showing 'der letzten 90 Tage' and a link to '> Übersicht aller Sendungen'. The bottom one is 'Verfolgen' (Track), with a text box containing 'Bis zu 10 Nummern möglich, bitte mit Komma oder Enter trennen' and a 'Verfolgen' button.

Und jetzt?

- Das Excelfile mit Makro ist günstiger im Betrieb
- Kein Manager bei DHL hat das Interesse das weg zu machen.
 - Ist günstiger, das File zu verschlüsseln, damit kein Virenschanner den code lesen kann.
 - «Erweiterte Sicherheitsvorkehrungen im Bereich Datenschutz» - wissenschon...
- DHL ist damit Teil des Problems

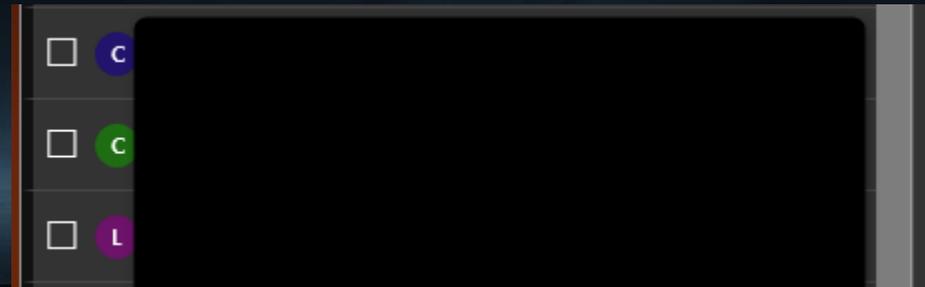
Und jetzt?

- Entscheider müssen aufhören, xlsx als Lösung zu wählen
- Es gibt wenig finanzielle Anreize und Sie haben ja keinen Schaden
- Stattdessen tragen DHL & Co weiter zur Abwärtsspirale bei.



BIMI, VMC, is nich ok

- Neu gibt es VMC – «Verified Mark Certificates
- Damit kann – wenn ihr euer Logo als Marke eingetragen habt –
- Euer Mailclient dann statt einem Runden logo das Logo des Absenders anzeigen



Die Betrüger freuts...

- Neu werden Accounts welche kompromittiert und mit BIMl und VMC zertifiziert sind halt teurer gehandelt in den Datenbörsen.
- Das kompromittieren von Accounts von sauber eingerichteten Domains – deren User noch keine Passkeys verwenden – wird immer lohnender.

Vielen Dank für eure Aufmerksamkeit