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

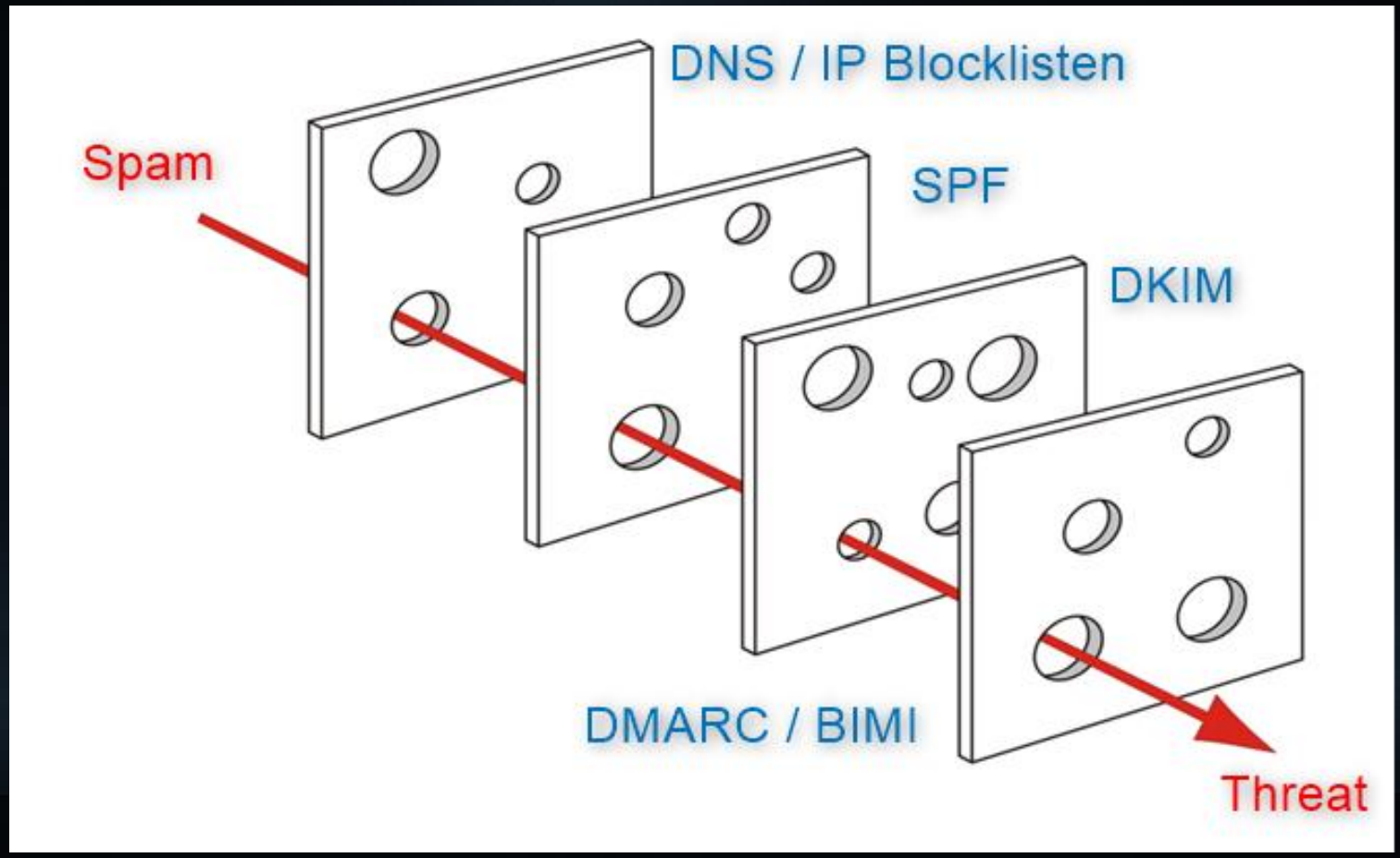
BEC?

- 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 Pflästerli
- 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

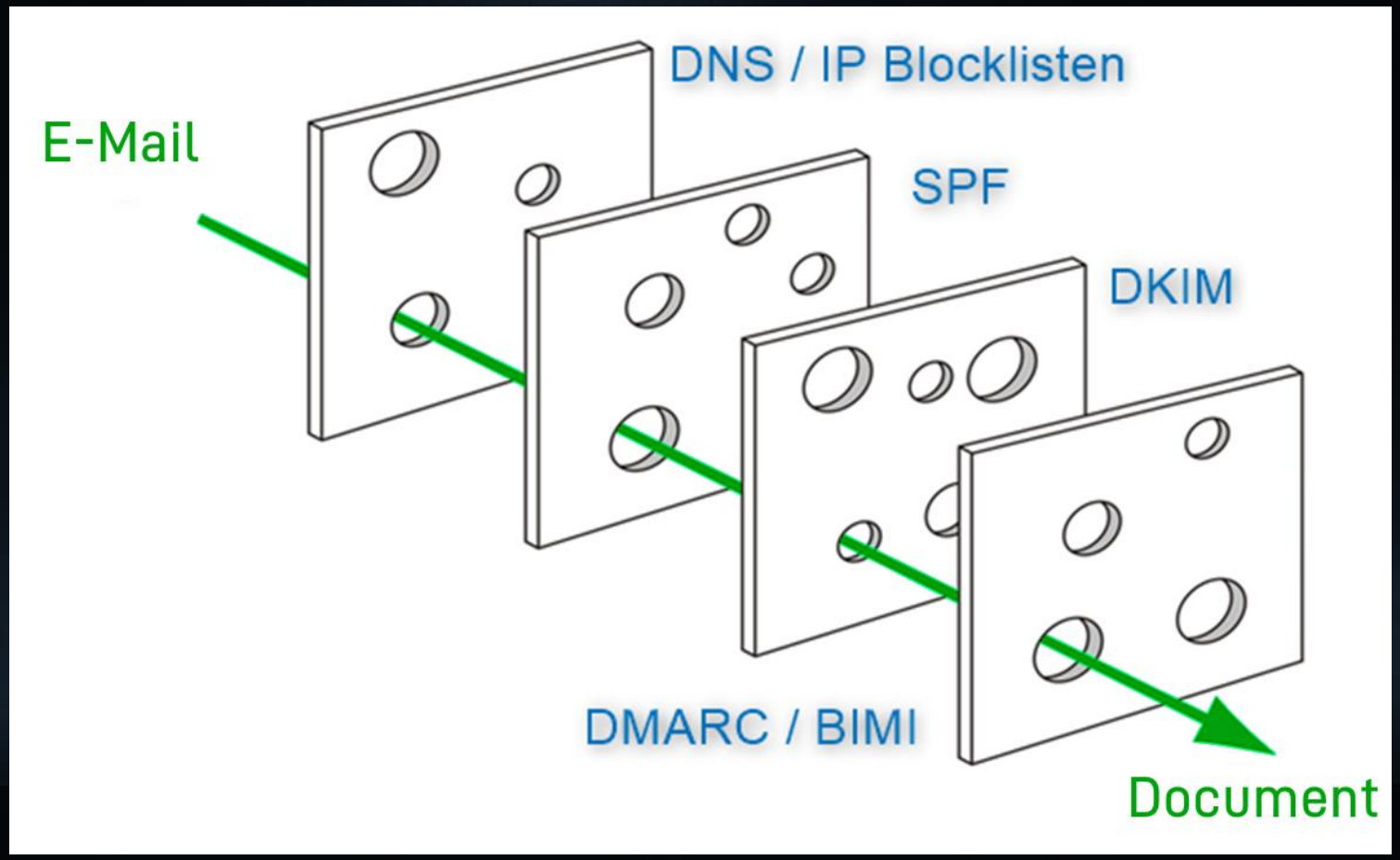
TCP / IP / DNS	Grundlagen
SMTP	Grundlagen
SSL / TLS	Sicherheit
DNSBL	Externer Ruf
Graylisting	Verzögerung
SPF	Selbstdeklarativ
DKIM	Absendersignatur
DMARC	Selbstdeklarativ
Spam-Filter	Mustererkennung
Antivirus	Signaturerkennung

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

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

Antworten | Allen antworten | Weiterleiten | ...

Mo. 07.04.2025 10:19

[redacted]

[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

Preisanfrage 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

Echt oder Fake?

DHL, XLS , ihr könnt mich mal

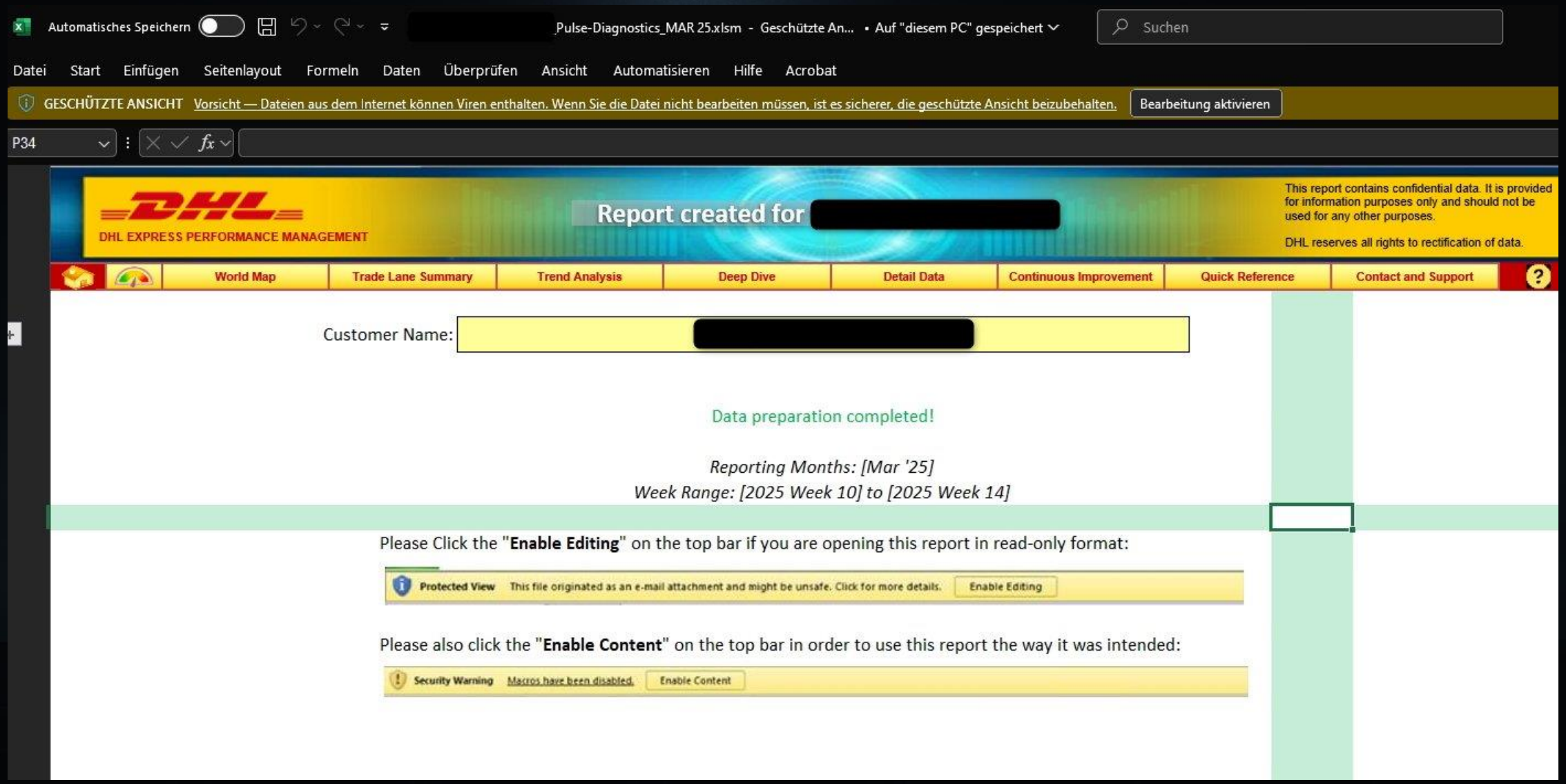
Person als Absender	Vertrauen schaffen? Manueller Versand?
Excel mit Makros im Anhang	Warum Makros?
Verschlüsselung mit Passwort	Obfuscation (Antivirus / Anti-Spam)
Telefonnummer: Handynummer	Warum keine Haupt oder Direktnummer?
Kontaktlink: dhl.com	Scheint legitim
Preisanfrage: emlfiles4.com	Was ist das für eine URL?

Anhang öffnen oder nicht?

Zwischenstand

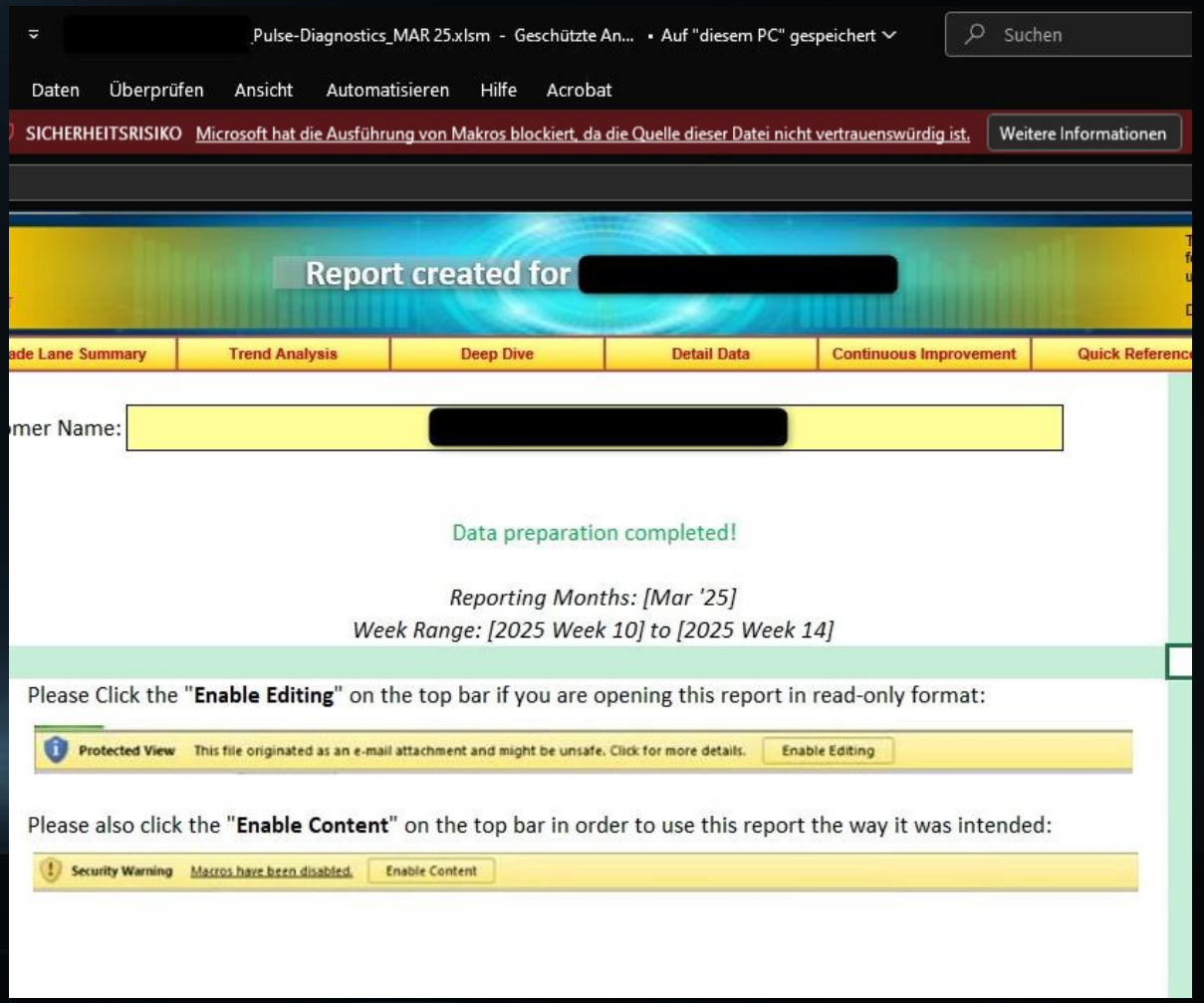
- Mindestens 7 technische Hürden mussten überwunden werden
- 2-3 Vertrauensmassnahmen: Versand durch Betreuer, Mobil-Nr direkt & Kontaktinfos von DHL.com herunterladbar.
- Nun kann die Datei geöffnet werden!

DHL, XLS, ihr könnt mich mal

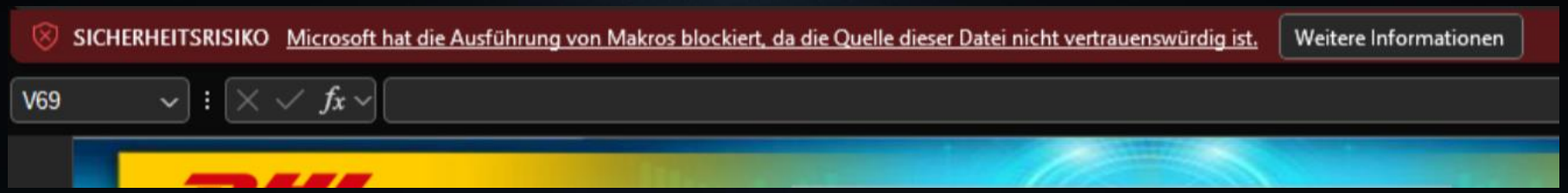


DHL, XLS , ihr könnt mich mal

- Mark of the Web: Makros aus!
- Bearbeitungsschutz: Office
- «Inhalt aktivieren»: Makrosicherheit



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 (Rechtklick > 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.

https://www.fhnw.ch/de/die-fhnw/hochschulen/hsw/media-newsroom/news/die-cyberstudie-2024-dreiteilige-befragung-der-schweizer-kmu-bevoelkerung-und-it-dienstleistungsunternehmen

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 auschalten.

BEC

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

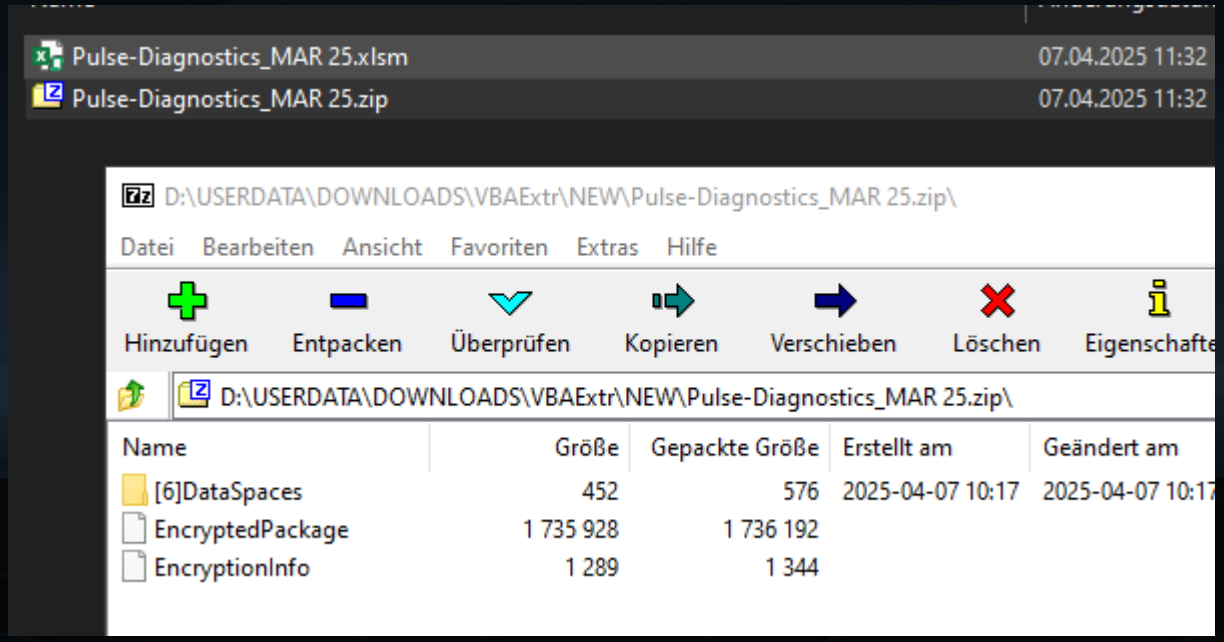
Zwischenstand

- 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...

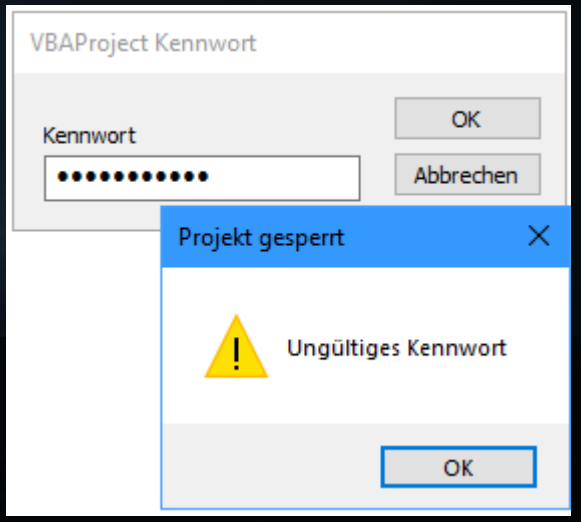


ZIP, DPB und HxD

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

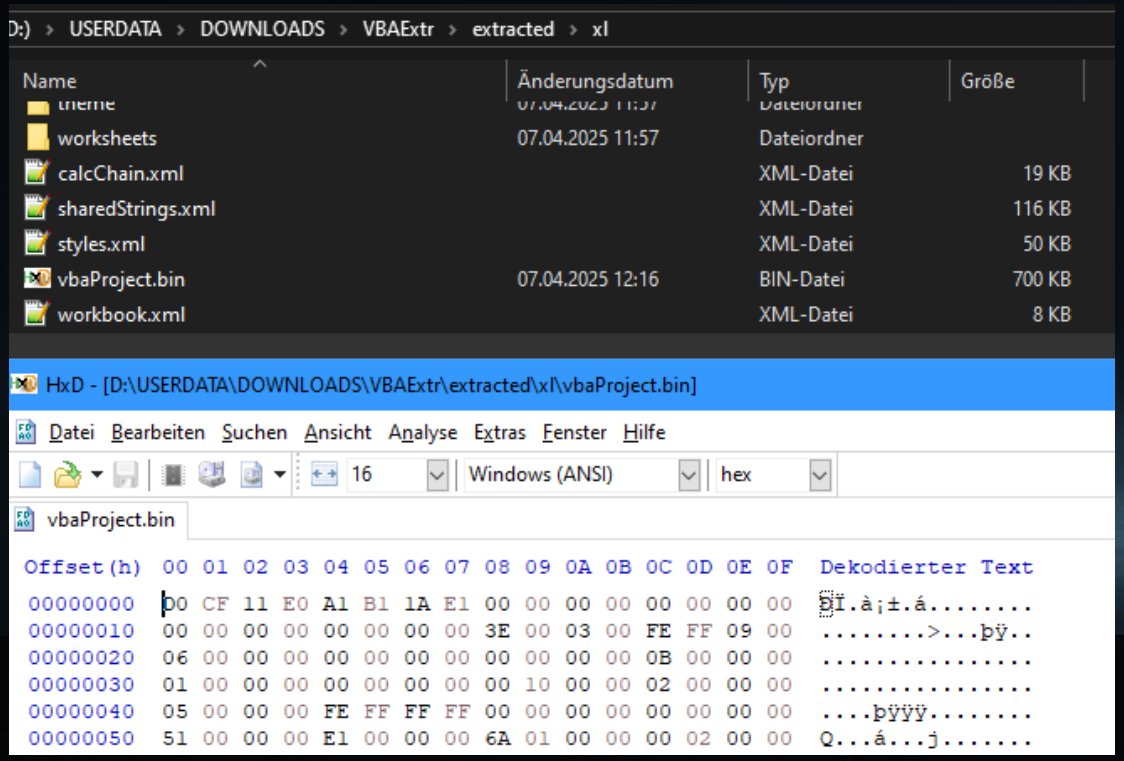
Achtung – aufgrund erweiterter Sicherheitsvorkehrungen im Bereich Datenschutz wird der Report verschlüsselt an Sie versendet. Das Passwort zum Öffnen des Files lautet [redacted] Danach erhalten Sie wie üblich Zugriff und Einsicht.

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



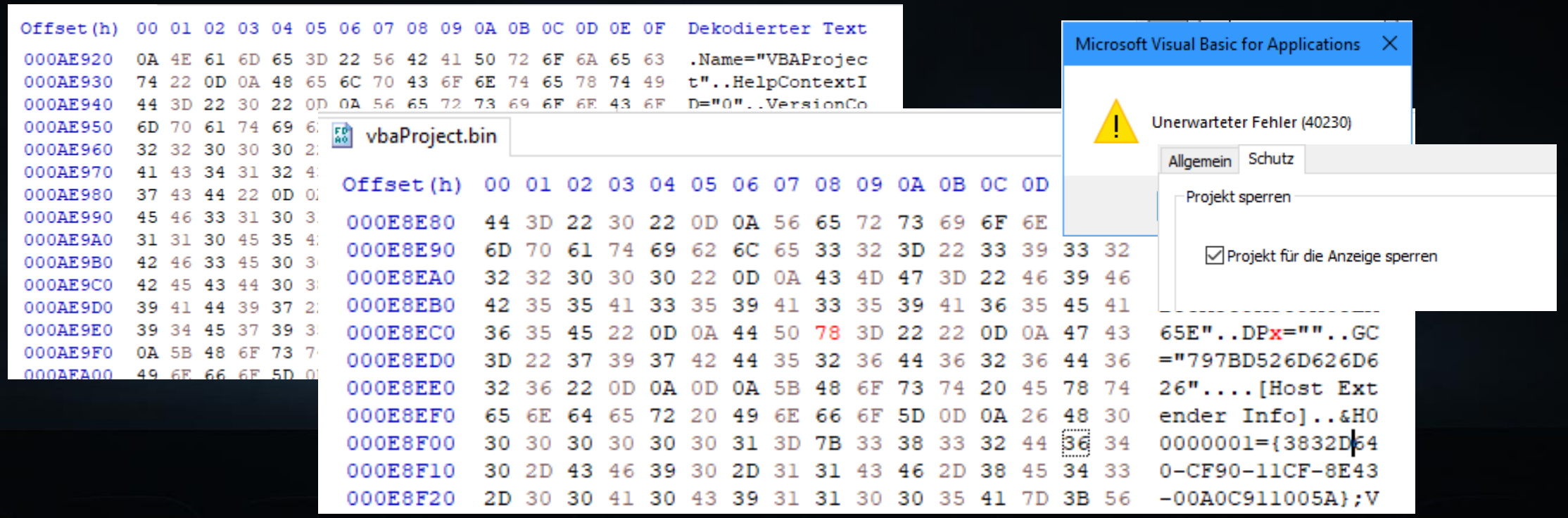
ZIP, DPB und HxD

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



ZIP, DBP und HxD

- Einmal den Begriff DPB suchen…
- und den DP**B** mit DP**x** ersetzen



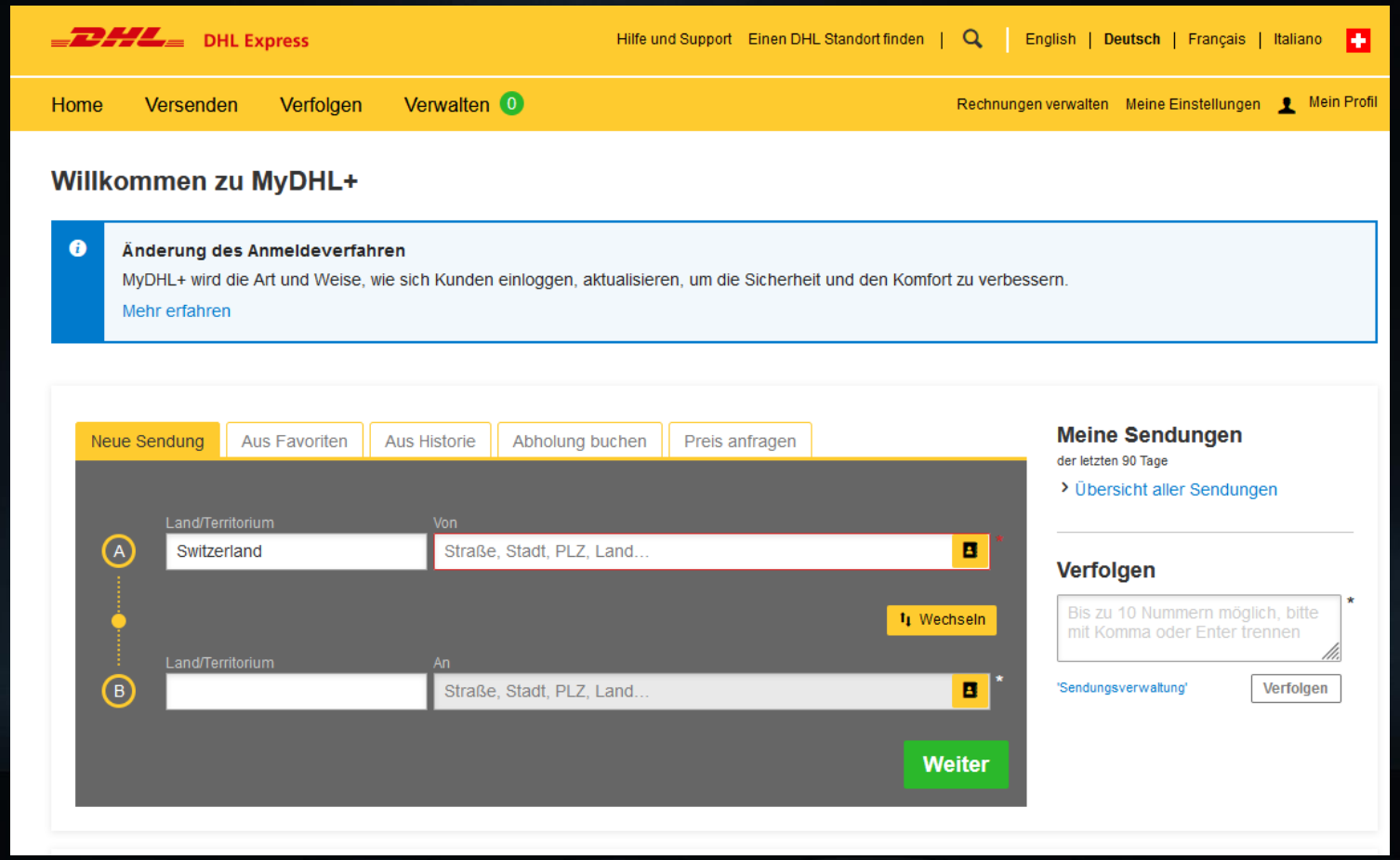
Wofür das alles?

SQL, VBS, tatatata

```
        str_date = str_date & " OR ([Startclock Year] = " & Left(Sheets("LOV").Cells(3, 14).Value, 4) & " AND [Startclock Month] = '" & Sheets("
'Ap     str_date = str_date & " OR ([Startclock Year] = " & Left(Sheets("LOV").Cells(4, 14).Value, 4) & " AND [Startclock Month] = '" & Sheets("
' A     str_date = str_date & " OR ([Startclock Year] = " & Left(Sheets("LOV").Cells(5, 14).Value, 4) & " AND [Startclock Month] = '" & Sheets("
I       str_date = str_date & " OR ([Startclock Year] = " & Left(Sheets("LOV").Cells(6, 14).Value, 4) & " AND [Startclock Month] = '" & Sheets("
I       str_date = str_date & " OR ([Startclock Year] = " & Left(Sheets("LOV").Cells(7, 14).Value, 4) & " AND [Startclock Month] = '" & Sheets("
I       Else
A        If Sheets("Dashboard").Range("C7").Value = "Full Period" Then
D        str_date = " "
A        End If
         End If
         End If
E        End If
A        End If
S        End If

D        'Services and Net
A        strmainval = "Sum([Count of Shipments]),Sum([Net Monitored Volume]),sum([DHL Controllable Delay Flag])"
E        str_fields = "[" & SvcValue & "]"
         strrow = Application.WorksheetFunction.CountA(Sheets("Raw_Data").Range("C:C"))

I
I        ConnString = "Provider=Microsoft.ACE.OLEDB.12.0;Data Source=" & GetLocalPath(ThisWorkbook.Path) & "\" & ThisWorkbook.Name & " ;Extended
S        Set oCn = New ADODB.Connection
E        oCn.ConnectionString = ConnString
I        oCn.Open
S
E        SQL = ""
E        SQL = SQL & " SELECT " & str_fields & ", " & strmainval
E        SQL = SQL & " FROM [Raw_Data$" ' & ctsheet
         SQL = SQL & "] WHERE " & str_product_filter & " " & str_date & " GROUP BY " & str_fields & " order by Sum([Count of Shipments]) DESC "

E        Set oRS = New ADODB.Recordset
         oRS.Source = SQL
         oRS.ActiveConnection = oCn
End
         oRS.CursorLocation = adUseClient
         oRS.CursorType = adOpenStatic
```

Wie kommt das?

Gäbe es nicht bessere Methoden?

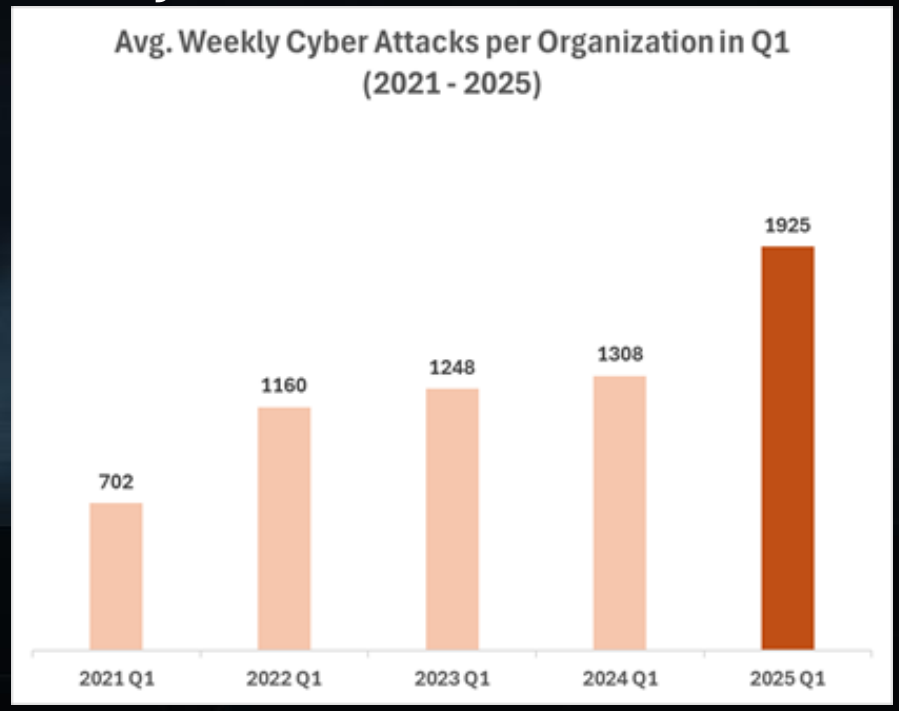


Und jetzt?

- 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 Virenscanner den code lesen kann.
  - «Erweiterte Sicherheitsvorkehrungen im Bereich Datenschutz» - wissenschon…
- DHL ist damit Teil des Problems

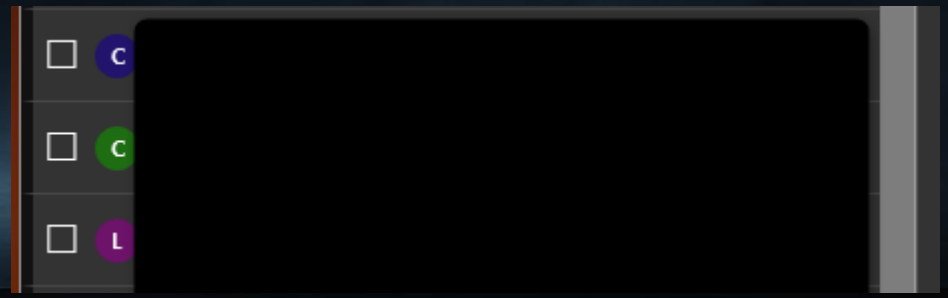
Und jetzt?

- Entscheider müssen aufhören, xlsm 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 BIMI 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