1
00:00:14,400 --> 00:00:17,200
Om mee te blijven met de veranderingen
in je werkomgeving

2
00:00:17,233 --> 00:00:19,266
moet je continu leren en groeien.

3
00:00:19,533 --> 00:00:23,633
Met de opleidingen en begeleiding
van Cevora scherp je als bediende

4
00:00:23,700 --> 00:00:26,966
je kennis en vaardigheden aan
doorheen je loopbaan.

5
00:00:27,133 --> 00:00:28,866
Zo blijf je sterk werk leveren.

6
00:00:29,500 --> 00:00:33,700
Dirk geeft al meer dan twintig jaar
vol passie les in technische onderwerpen.

7
00:00:33,833 --> 00:00:39,000
Als IT-trainer en systeembeheerder
maakt hij complexe materie begrijpelijk.

8
00:00:39,433 --> 00:00:43,366
De laatste jaren heeft hij zich
gespecialiseerd in Microsoft 365

9
00:00:43,466 --> 00:00:44,700
voor eindgebruikers

10
00:00:44,766 --> 00:00:47,500
met een essentiële focus op cybersecurity.

11
00:00:47,900 --> 00:00:52,466
In de volgende 30 minuten deelt Dirk
zijn unieke inzichten en praktische tips

12
00:00:52,500 --> 00:00:55,733
om jou te beschermen

tegen de gevaren van het internet.

13
00:00:56,933 --> 00:01:00,133
Welkom bij de Learning Snack
rond cybersecurity.

14
00:01:00,200 --> 00:01:01,366
Ik ben Dirk Tielens

15
00:01:01,433 --> 00:01:05,333
en ik ga je vandaag
een beetje meer tips proberen te geven

16
00:01:05,500 --> 00:01:07,800
om je wat veiliger te voelen

17
00:01:08,400 --> 00:01:09,933
in de digitale wereld.

18
00:01:10,066 --> 00:01:13,133
We gaan dat doen in drie topics,
drie paragrafen.

19
00:01:13,333 --> 00:01:14,666
Eerst en vooral gaan we kijken:

20
00:01:14,733 --> 00:01:17,466
Is het wel noodzakelijk
om je te beschermen

21
00:01:17,533 --> 00:01:18,600
in deze digitale wereld?

22
00:01:18,666 --> 00:01:20,500
Dus, waarom moet ik mij beschermen?

23
00:01:21,400 --> 00:01:24,966
In een tweede topic gaan we kijken
wat er allemaal kan mislopen.

24
00:01:25,866 --> 00:01:27,833
Wat kan je overkomen?

25
00:01:28,033 --> 00:01:30,466
Ransomware bijvoorbeeld is
daar een bekend voorbeeld van,

26
00:01:30,533 --> 00:01:32,900
dan moet je data versleuteld worden.

27
00:01:33,300 --> 00:01:36,200
En ten slotte geef ik je nog graag
wat tips en tricks mee

28
00:01:36,300 --> 00:01:37,733
hoe je je kan beschermen

29
00:01:38,000 --> 00:01:40,266
tegen al die digitale gevaren.

30
00:01:41,300 --> 00:01:44,533
Eerst misschien eens overlopen
waarom het zo noodzakelijk is

31
00:01:45,000 --> 00:01:48,633
om toch enige vorm
van digitale bescherming te voorzien.

32
00:01:49,366 --> 00:01:51,200
Ik zou graag willen beginnen
met een quote,

33
00:01:51,566 --> 00:01:56,366
namelijk dat amateurs systemen hacken

34
00:01:56,433 --> 00:01:58,500
en dat professionals mensen hacken.

35
00:01:58,900 --> 00:02:02,633
En dat laatste is wat je vandaag
meer en meer ziet gebeuren.

36
00:02:02,700 --> 00:02:05,633
Juist omwille van het feit

dat de eindgebruikers, de mensen

37
00:02:05,866 --> 00:02:07,966
de zwakste schakel in de keten worden

38
00:02:08,000 --> 00:02:12,000
in die zin dat de systemen veel veiliger
geworden zijn dan vroeger

39
00:02:12,166 --> 00:02:13,666
en dat systemen hacken

40
00:02:14,166 --> 00:02:16,466
eigenlijk moeilijker en moeilijker
wordt voor hackers.

41
00:02:16,533 --> 00:02:21,733
Vandaar dat ze vooral die mensen aanvallen
of zich gaan richten tot de mensen

42
00:02:21,966 --> 00:02:25,433
om op die manier
inloggegevens bijvoorbeeld te bekomen

43
00:02:25,500 --> 00:02:30,466
of die dubbele authenticatie, die code
die bij bankverrichtingen gevraagd wordt

44
00:02:30,766 --> 00:02:33,966
en op die manier
toegang te krijgen tot de systemen.

45
00:02:34,266 --> 00:02:36,033
Dus wat vroeger gebeurde,

46
00:02:36,066 --> 00:02:38,633
dat de virussen Windows
niet meer lieten opstarten,

47
00:02:38,766 --> 00:02:41,000
dat is een beetje passé op dit moment.

48

00:02:42,866 --> 00:02:44,300
Waarom je je ook moet beschermen,

49
00:02:44,366 --> 00:02:46,900
is omdat meer en meer data
tegenwoordig in de cloud staat.

50
00:02:47,200 --> 00:02:49,000
Vroeger hadden we de on-premise omgevingen

51
00:02:49,066 --> 00:02:51,066
dus dat alle data
binnen het bedrijf stond

52
00:02:51,133 --> 00:02:52,966
en dan moest je al fysieke toegang hebben

53
00:02:53,166 --> 00:02:54,366
om aan die data te kunnen.

54
00:02:54,533 --> 00:02:55,900
Vandaag staat alles in de cloud.

55
00:02:55,966 --> 00:02:57,600
Heel interessant voor de eindgebruiker

56
00:02:57,666 --> 00:03:01,033
want die kan uiteraard van overal
aan zijn of haar data.

57
00:03:01,333 --> 00:03:04,033
Maar ook interessant voor de hacker
want die kan dat ook.

58
00:03:04,433 --> 00:03:05,633
En daar komt ook nog bij

59
00:03:05,700 --> 00:03:10,133
dat we al dan niet bewust
heel veel informatie over onszelf delen

60
00:03:10,200 --> 00:03:11,366

via sociale media.

61
00:03:11,400 --> 00:03:14,166
En die informatie is uiteraard
voor hackers ook interessant.

62
00:03:14,466 --> 00:03:16,933
Denk maar aan de geboortedatum
van onze kinderen

63
00:03:17,100 --> 00:03:18,500
of de naam van onze huisdieren

64
00:03:18,666 --> 00:03:22,033
die we zelf vaak al dan niet bewust
in ons paswoord verwerken.

65
00:03:22,166 --> 00:03:24,266
En dat maakt het voor hackers
al wat makkelijker

66
00:03:24,333 --> 00:03:26,233
om toegang te krijgen tot die gegevens.

67
00:03:28,466 --> 00:03:32,400
Uit statistieken blijkt ook
dat 95% van alle cyberincidenten

68
00:03:32,466 --> 00:03:34,566
veroorzaakt wordt door menselijke fouten.

69
00:03:34,766 --> 00:03:36,100
Wat zijn die menselijke fouten?

70
00:03:36,166 --> 00:03:39,300
Wel, dan gaat het vooral over phishing,
dus het hengelen naar gegevens,

71
00:03:39,466 --> 00:03:41,733
de sms'jes of de mails
die je krijgt met de vraag

72

00:03:42,133 --> 00:03:43,900
om dringend je paswoord te veranderen.

73
00:03:44,366 --> 00:03:47,800
AI gaat daar trouwens in de toekomst
een zeer belangrijke rol in spelen,

74
00:03:47,933 --> 00:03:49,033
komen we later op terug.

75
00:03:50,200 --> 00:03:53,500
Maar bijvoorbeeld zwakke wachtwoorden
zijn ook heel vaak de oorzaak

76
00:03:53,566 --> 00:03:54,900
van cyberincidenten.

77
00:03:55,300 --> 00:03:56,766
Apparaten die verloren geraken.

78
00:03:56,833 --> 00:03:59,400
Denk maar aan de laptop
die je vergeet op de trein.

79
00:04:00,266 --> 00:04:02,700
Of onvoldoende kennis,
onvoldoende opleiding.

80
00:04:03,233 --> 00:04:07,066
Mensen die bijvoorbeeld een bestand
beschikbaar stellen voor externen

81
00:04:07,133 --> 00:04:09,766
maar dat dan onbewust
voor de hele wereld beschikbaar stellen

82
00:04:09,800 --> 00:04:13,200
in plaats van enkel
voor die specifieke personen.

83
00:04:13,900 --> 00:04:14,933
En tot slot ...

84
00:04:15,400 --> 00:04:18,700
Het onveilige gebruik
van openbare wifinetwerken.

85
00:04:18,766 --> 00:04:21,333
Wanneer je op een openbaar wifinetwerk
inlogt

86
00:04:21,866 --> 00:04:25,366
is het zo dat alle informatie
die je verzendt,

87
00:04:25,433 --> 00:04:29,666
dat die meegelezen kan worden door
wie toegang heeft tot dat wifinetwerk.

88
00:04:29,700 --> 00:04:31,800
En als er dan
geen extra vorm van beveiliging is,

89
00:04:31,933 --> 00:04:34,100
als die data niet extra versleuteld is,

90
00:04:34,533 --> 00:04:36,633
dan kan je gewoon meelezen

91
00:04:36,966 --> 00:04:39,100
en dat is uiteraard ook niet de bedoeling.

92
00:04:41,833 --> 00:04:45,700
We hebben dus een concreet voorbeeld
uitgewerkt waaruit moet blijken

93
00:04:45,766 --> 00:04:49,266
dat het toch wel belangrijk is dat je
een zekere bescherming aan de dag legt.

94
00:04:49,566 --> 00:04:52,066
En we hebben dat eens bekeken
met een voorbeeld

95
00:04:52,166 --> 00:04:54,533

van een Microsoft 365 schooltenant.

96
00:04:54,800 --> 00:04:55,866
Wat is een tenant?

97
00:04:55,933 --> 00:04:58,466
Dat is de Microsoft-omgeving
van een organisatie,

98
00:04:58,500 --> 00:04:59,833
dus in dit geval de school.

99
00:05:00,300 --> 00:05:04,833
En die school bestaat uit 2800 leerlingen
en een 600-tal personeelsleden,

100
00:05:04,866 --> 00:05:07,900
dus in totaal zo'n 3400 gebruikers.

101
00:05:08,300 --> 00:05:12,966
En we hebben, na het deactiveren
van extra bescherming,

102
00:05:13,033 --> 00:05:16,266
zoals dat gebruikers
niet van overal mogen inloggen,

103
00:05:16,433 --> 00:05:18,733
dus we hebben de beveiliging
een beetje lager gezet.

104
00:05:18,833 --> 00:05:21,966
Gebruikers mochten
van eender waar ter wereld inloggen

105
00:05:22,000 --> 00:05:23,766
en we hebben gekeken wat dat geeft

106
00:05:24,400 --> 00:05:25,400
op een feestdag

107
00:05:25,533 --> 00:05:28,066

op een pinkstermaandag
gedurende een vijftal minuten.

108
00:05:28,633 --> 00:05:31,966
En de resultaten die daar uitkwamen
zijn toch enigszins verontrustend.

109
00:05:32,433 --> 00:05:37,166
We hebben gezien dat daar ongeveer
10.000 mislukte inlogpogingen gebeurd zijn

110
00:05:37,600 --> 00:05:39,566
op 41 accounts.

111
00:05:39,700 --> 00:05:41,533
Waarom specifiek 41 accounts?

112
00:05:41,700 --> 00:05:45,300
Dat zijn accounts van gebruikers
wiens e-mailadres gekend is

113
00:05:45,366 --> 00:05:49,233
en hackers hebben gewoon geprobeerd
om in die accounts binnen te geraken.

114
00:05:49,366 --> 00:05:52,733
Voor alle duidelijkheid, ze zijn
in geen enkel account binnengeraakt,

115
00:05:52,900 --> 00:05:54,666
maar ze hebben wel een poging ondernomen.

116
00:05:55,133 --> 00:05:58,633
Het ging zelfs zo ver
dat binnen die 5 minuten op één account

117
00:05:58,700 --> 00:06:02,000
1220 keer geprobeerd is
om in te loggen.

118
00:06:03,766 --> 00:06:06,433
Er waren zelfs zes accounts van die 41

119
00:06:06,566 --> 00:06:08,666
waar men binnen die 5 minuten

120
00:06:08,966 --> 00:06:11,766
meer dan 1000 keer geprobeerd heeft.

121
00:06:12,266 --> 00:06:13,333
Toevallig waren dat ook

122
00:06:14,100 --> 00:06:17,433
accounts van personeelsleden
en zelfs één directielid.

123
00:06:18,800 --> 00:06:21,266
De aanvallen kwamen vanuit alle kanten,

124
00:06:21,766 --> 00:06:24,066
vanuit 108 landen om precies te zijn,

125
00:06:24,133 --> 00:06:27,100
maar heel concreet,
de meeste kwamen uit China, Zuid-Korea,

126
00:06:27,600 --> 00:06:30,166
dan de Verenigde Staten, Hongkong

127
00:06:30,366 --> 00:06:33,266
en tot slot
de Verenigde Arabische Emiraten.

128
00:06:35,200 --> 00:06:38,400
Nu, als we eens kijken,
als we dan toch het slachtoffer worden,

129
00:06:38,500 --> 00:06:40,800
wat kan er allemaal mislopen?

130
00:06:40,866 --> 00:06:42,133
Wat kan er fout gaan?

131
00:06:42,666 --> 00:06:46,033

Wel, wat vandaag het meest voorkomt,

132
00:06:46,333 --> 00:06:47,533
is verlies van data.

133
00:06:47,866 --> 00:06:50,200
Verlies van data, vooral door ransomware.

134
00:06:50,266 --> 00:06:52,933
Ransomware is software die je,

135
00:06:53,966 --> 00:06:58,133
door een softwarepakketje te installeren
van een malafide site,

136
00:06:58,766 --> 00:07:00,600
die je data gaat versleutelen.

137
00:07:01,233 --> 00:07:04,166
Dat wil zeggen
dat je persoonlijke bestanden, je foto's,

138
00:07:04,233 --> 00:07:07,500
je documenten enz.
gewoon onbruikbaar worden.

139
00:07:07,600 --> 00:07:11,700
Ze worden in een soort van kistje gestoken

140
00:07:11,966 --> 00:07:13,733
dat wordt afgesloten door de hacker

141
00:07:13,933 --> 00:07:16,233
en als je die softwarematige sleutel
niet hebt,

142
00:07:16,300 --> 00:07:18,133
kan je daar niets meer mee doen.

143
00:07:18,433 --> 00:07:21,600
Het bekendste slachtoffer
van zo'n ransomwareaanval

144
00:07:21,666 --> 00:07:22,966
is de stad Antwerpen.

145
00:07:23,233 --> 00:07:26,700
Diest en Zwijndrecht zijn
ook slachtoffer geworden.

146
00:07:27,433 --> 00:07:29,400
Duvel, nog niet zo lang geleden.

147
00:07:29,600 --> 00:07:32,400
En uiteraard nog een hele hoop andere.

148
00:07:32,633 --> 00:07:35,600
Maar als je dit aan de hand krijgt
en je hebt geen deftige back-up

149
00:07:36,033 --> 00:07:38,333
dan heb je een serieus probleem.

150
00:07:40,866 --> 00:07:45,233
Veeam, een bekende softwarefabrikant
van back-upsoftware,

151
00:07:45,300 --> 00:07:49,100
heeft zelfs een enquête georganiseerd
onder zo'n 12.000 gebruikers

152
00:07:49,200 --> 00:07:51,266
die slachtoffer werden
van zo'n cyberaanval.

153
00:07:51,600 --> 00:07:53,033
Daaruit is gebleken

154
00:07:53,433 --> 00:07:58,033
dat 41% van al hun data
die aangevallen wordt

155
00:07:58,700 --> 00:08:04,100
dat daar maar 57%

hersteld van kan worden.

156
00:08:04,866 --> 00:08:09,733
Dus als er een aanval gebeurt,
41% van alle data gaat versleuteld zijn

157
00:08:10,033 --> 00:08:12,166
en van die versleutelde data

158
00:08:12,666 --> 00:08:17,500
kan slechts een goede 2/3
of bijna 2/3 hersteld worden.

159
00:08:17,766 --> 00:08:22,666
Dat zijn hallucinante cijfers
die je misschien toch wel doen nadenken.

160
00:08:23,800 --> 00:08:27,133
En ook een paar cijfers
waar ik zelf wat van schrok,

161
00:08:27,166 --> 00:08:29,866
dat vier op vijf betaalt

162
00:08:30,333 --> 00:08:31,600
om data terug te krijgen.

163
00:08:31,666 --> 00:08:33,833
Het is geen garantie dat je
met zo'n ransomware

164
00:08:33,900 --> 00:08:36,133
je data effectief terug gaat krijgen.

165
00:08:36,233 --> 00:08:40,433
Dat zie je wat lager: 1 op 3 slachtoffers
kon hun data zelfs niet herstellen.

166
00:08:40,733 --> 00:08:41,733
Maar ...

167
00:08:41,800 --> 00:08:44,133

vreemd genoeg blijkt
dat de meeste bedrijven,

168
00:08:44,200 --> 00:08:46,066
waarschijnlijk om economische redenen,

169
00:08:46,266 --> 00:08:47,866
toch nog steeds betalen

170
00:08:48,166 --> 00:08:51,366
als ze slachtoffer worden
van zo'n ransomwareaanval.

171
00:08:54,733 --> 00:08:56,133
Wat kan er nog fout gaan?

172
00:08:56,600 --> 00:09:00,100
Dat is dat iemand toegang krijgt tot data

173
00:09:00,166 --> 00:09:02,566
of dat je data
ongeoorloofd verspreid wordt.

174
00:09:02,633 --> 00:09:05,300
Dus naast dat verlies,
waar we het zonet over gehad hebben,

175
00:09:05,800 --> 00:09:07,333
kan je ook aan de hand krijgen

176
00:09:07,400 --> 00:09:10,633
dat je data op het internet belandt
en dat je dat liever niet hebt.

177
00:09:10,766 --> 00:09:12,466
Gebeurt heel vaak via die phishing,

178
00:09:12,666 --> 00:09:17,433
denk maar aan hackers
die toegang krijgen tot je bankgegevens.

179
00:09:17,433 --> 00:09:19,866

AI gaat hier
een belangrijke rol in spelen.

180
00:09:20,000 --> 00:09:23,566
We kennen allemaal
het sms'je van zoonlief of dochterlief

181
00:09:23,733 --> 00:09:26,433
waarin gevraagd wordt
om dringend een overschrijving te doen.

182
00:09:27,300 --> 00:09:28,333
Wel ...

183
00:09:28,633 --> 00:09:31,733
In de toekomst gaat
dochterlief of zoonlief je bellen.

184
00:09:31,933 --> 00:09:33,000
't Is te zeggen,

185
00:09:33,233 --> 00:09:35,800
ze gaan misschien
met de stem van zoonlief of dochterlief

186
00:09:35,900 --> 00:09:37,333
die ze vinden op het internet

187
00:09:38,200 --> 00:09:40,066
een andere boodschap monteren

188
00:09:40,133 --> 00:09:43,800
en op die manier gaan ze
je proberen wijs te maken

189
00:09:43,900 --> 00:09:45,966
dat je met je dochter belt
of met je zoon belt

190
00:09:46,233 --> 00:09:49,900
en dat je de codes
die ze nodig hebben doorgeeft.

191
00:09:50,433 --> 00:09:53,066
Ook deepfakevideo's gaan
een belangrijke rol spelen

192
00:09:53,200 --> 00:09:55,166
in phishing naar gegevens.

193
00:09:55,233 --> 00:09:58,466
En ook nieuw is polyforme malware.

194
00:09:58,533 --> 00:10:00,433
Malware is schadelijke software.

195
00:10:00,833 --> 00:10:05,033
En polyforme malware is malware
die zichzelf herschrijft

196
00:10:05,233 --> 00:10:10,066
zodanig dat die moeilijker detecteerbaar
wordt voor antivirussoftware.

197
00:10:12,466 --> 00:10:14,433
Een derde zaak die fout kan gaan

198
00:10:14,600 --> 00:10:18,933
naast verlies van data en
ongeoorloofde toegang

199
00:10:19,800 --> 00:10:21,433
is het lamleggen van systemen

200
00:10:22,533 --> 00:10:25,033
via bijvoorbeeld
zogenaamde DDoS-aanvallen.

201
00:10:25,100 --> 00:10:26,166
Wat zijn dat?

202
00:10:26,233 --> 00:10:29,666
Dat zijn zeer gerichte aanvallen
naar een systeem,

203
00:10:29,800 --> 00:10:32,766
dus niet zozeer meer naar
die eindgebruiker maar naar een systeem

204
00:10:32,833 --> 00:10:36,633
waardoor ze bijvoorbeeld
je internetverbinding kunnen uitschakelen.

205
00:10:37,100 --> 00:10:39,900
Het komt er eigenlijk op neer
dat ze bij een DDoS-attack

206
00:10:40,000 --> 00:10:45,066
zoveel data naar een systeem sturen
dat dat totaal onbruikbaar wordt.

207
00:10:45,166 --> 00:10:50,233
En je internetverbinding, je gaat merken
dat je internetverbinding wegvalt.

208
00:10:50,900 --> 00:10:53,500
Is bovendien zeer simpel uit te voeren.

209
00:10:53,533 --> 00:10:56,100
Ik ben daar zelf ook al
een aantal keren mee geconfronteerd.

210
00:10:56,566 --> 00:10:58,933
De jongste dader was bij mij 11 jaar.

211
00:10:59,100 --> 00:11:01,333
Die zat in het zesde leerjaar.

212
00:11:01,533 --> 00:11:03,200
Dus vooral scholen hebben hier last van

213
00:11:03,266 --> 00:11:06,400
want dat is natuurlijk
zeer interessant voor de kinderen

214
00:11:06,466 --> 00:11:09,733
om de internetverbinding

van de school tijdelijk plat te leggen.

215
00:11:10,300 --> 00:11:11,900
Je kan je hiertegen beschermen

216
00:11:12,133 --> 00:11:17,200
maar daar hangt een behoorlijk
prijskaartje aan vast.

217
00:11:17,700 --> 00:11:22,166
Maar als je daarmee geconfronteerd wordt,
is dat een zeer lastige situatie.

218
00:11:22,966 --> 00:11:25,833
Om een concreet voorbeeld te geven
van een DDoS-attack

219
00:11:25,933 --> 00:11:29,166
hebben we hier een monitor gestart
die een internetverbinding monitort.

220
00:11:29,400 --> 00:11:31,933
Je ziet in die grafiek op de tweede regel

221
00:11:32,200 --> 00:11:35,033
twee lijnen,
een groene en een blauwe lijn.

222
00:11:35,100 --> 00:11:38,766
Die groene, bovenste geeft aan
of de internetverbinding nog online is.

223
00:11:38,833 --> 00:11:41,300
Die blauwe geeft de responstijd weer.

224
00:11:41,433 --> 00:11:43,000
Dat is nu ongeveer 20 milliseconden.

225
00:11:43,033 --> 00:11:45,333
Onderaan kan je zien
dat de lijn nog altijd actief is

226

00:11:45,533 --> 00:11:47,300
en wanneer er een aanval wordt uitgevoerd

227
00:11:47,366 --> 00:11:50,633
en dat wordt nu vanop een site gedaan
die daar aan de rechterkant openstaat,

228
00:11:50,666 --> 00:11:51,666
ga je zien

229
00:11:51,933 --> 00:11:55,900
dat die internetverbinding
binnen afzienbare tijd naar beneden gaat

230
00:11:55,966 --> 00:11:58,466
en dat die internetverbinding
niet meer bereikbaar is.

231
00:11:58,533 --> 00:12:01,166
Je gaat dat zowel zien in de grafiek
als in de tabel

232
00:12:01,300 --> 00:12:03,100
en je ziet het hier vanonder in die tabel.

233
00:12:03,166 --> 00:12:05,433
Daar staat nu een aantal keren
'No internet connection'

234
00:12:05,566 --> 00:12:06,633
dus op dit moment

235
00:12:06,766 --> 00:12:10,733
zijn er een aantal laptops als bots

236
00:12:10,833 --> 00:12:14,566
naar die internetverbinding
zodanig veel data aan het sturen

237
00:12:14,900 --> 00:12:20,400
dat die gedurende een dertigtal seconden,
zal dat nu zijn, onbereikbaar is.

238
00:12:21,033 --> 00:12:23,133
En we zien ze ondertussen
al terug opkomen,

239
00:12:23,300 --> 00:12:25,233
zowel in de tabel onderaan
als in de grafiek.

240
00:12:25,600 --> 00:12:28,566
Het gaat nog een tijdje duren
eer die volledig gestabiliseerd is.

241
00:12:28,833 --> 00:12:33,733
Maar zoals je kan zien aan de rechterkant
op die tweede site die open staat,

242
00:12:34,000 --> 00:12:38,600
dat is niet meer dan een eenvoudige site
waar je een aantal gegevens moet ingeven

243
00:12:39,033 --> 00:12:44,300
en dan op SEND ATTACK klikken
om die internetverbinding lam te leggen.

244
00:12:46,233 --> 00:12:48,733
En een laatste zaak,
en die wordt vaak vergeten,

245
00:12:49,133 --> 00:12:51,333
dat zijn de gevaren van binnenuit.

246
00:12:52,366 --> 00:12:57,566
Ook een rancuneuze werknemer
kan een probleem vormen.

247
00:12:57,933 --> 00:13:00,700
Iemand die pas ontslagen wordt
en die denkt:

248
00:13:00,933 --> 00:13:05,600
Ik ben hier toch niet zo gelukkig,
ik ga nog mijn visitekaartje achterlaten.

249
00:13:06,533 --> 00:13:08,366
Dat kan voor heel wat problemen zorgen.

250
00:13:08,500 --> 00:13:10,533
Dus een account van een werknemer
bijvoorbeeld,

251
00:13:10,733 --> 00:13:13,766
die niet afgesloten is
na zijn ontslag of zijn vertrek.

252
00:13:14,200 --> 00:13:15,266
Ik merk heel vaak

253
00:13:15,700 --> 00:13:19,766
dat in sommige organisaties mensen die al
ettelijke maanden niet meer actief zijn,

254
00:13:19,866 --> 00:13:22,066
dat die blijkbaar toch nog
in hun account kunnen.

255
00:13:23,000 --> 00:13:25,266
Een medewerker, ik heb er
daarstraks al over verteld,

256
00:13:25,333 --> 00:13:27,433
een medewerker
die zijn data openbaar deelt

257
00:13:27,533 --> 00:13:30,766
dus openzet voor de hele wereld
in plaats van voor specifieke mensen.

258
00:13:31,633 --> 00:13:33,900
En misschien een handige tip daarbij
als laatste is:

259
00:13:33,933 --> 00:13:35,766
vermijd gedeelde accounts of wachtwoorden.

260
00:13:35,833 --> 00:13:37,333

We zien al te vaak dat

261
00:13:37,566 --> 00:13:40,033
een bepaalde account
door meerdere mensen gebruikt wordt.

262
00:13:40,100 --> 00:13:43,233
Daar heb je totaal geen controle over
wie die gegevens effectief heeft

263
00:13:43,266 --> 00:13:45,966
want die worden
heel makkelijk doorgegeven.

264
00:13:46,133 --> 00:13:47,766
Denk maar aan een wifipaswoord.

265
00:13:49,033 --> 00:13:51,866
Als één of twee mensen dat hebben
dan is het een kwestie van tijd

266
00:13:51,933 --> 00:13:56,233
vooraleer de hele organisatie
of wie het niet moet hebben

267
00:13:56,566 --> 00:13:58,833
ook over dat wifipaswoord beschikt.

268
00:14:00,666 --> 00:14:02,566
Dat zijn zo de dingen
die fout kunnen lopen,

269
00:14:02,633 --> 00:14:04,666
maar wat kan je daar zelf nu tegen doen?

270
00:14:04,733 --> 00:14:07,600
Uiteraard speelt IT zelf
hier een grote rol in.

271
00:14:07,666 --> 00:14:09,933
Ze vangen al een heel stuk op,

272

00:14:10,033 --> 00:14:13,300
maar als eindgebruiker kan je
ook nog jezelf beschermen

273
00:14:13,600 --> 00:14:15,700
tegen een aantal gevaren.

274
00:14:16,200 --> 00:14:21,833
De belangrijkste en meest bekende is
uiteraard de Multi-Factor Authentication.

275
00:14:21,933 --> 00:14:25,000
Multi-Factor Authentication wil
heel simpel zeggen

276
00:14:25,433 --> 00:14:29,333
dat je je op meer dan één manier
gaat identificeren,

277
00:14:29,433 --> 00:14:33,533
dus je gaat die identiteit
op meer dan één manier bewijzen.

278
00:14:33,866 --> 00:14:37,200
De bekendste voorbeelden zijn
Microsoft en Google Authenticator.

279
00:14:37,433 --> 00:14:41,533
Dat is een soort van code
die je op je gsm moet opvragen

280
00:14:41,600 --> 00:14:42,866
op het moment dat je inlogt

281
00:14:43,133 --> 00:14:48,100
en dat bewijst dat je de gsm
van de gebruiker in handen hebt

282
00:14:48,266 --> 00:14:52,100
want die code kan je alleen
op die ene specifieke gsm opvragen.

283
00:14:52,233 --> 00:14:54,366

Dat maakt het voor hackers
dus al wat moeilijker.

284
00:14:54,433 --> 00:14:56,933
Dus mochten ze dan beschikken
over je paswoord

285
00:14:57,266 --> 00:14:59,666
dan moeten ze die code op die gsm
ook nog ingeven

286
00:14:59,733 --> 00:15:03,033
en als ze dan niet beschikken over je gsm,
kunnen ze in principe niet binnen.

287
00:15:03,366 --> 00:15:06,166
De code komt soms ook binnen via sms.

288
00:15:07,133 --> 00:15:08,766
En een heel handige manier

289
00:15:10,200 --> 00:15:13,733
die zowel gebruiksgemak
als beveiliging combineert

290
00:15:13,933 --> 00:15:15,533
en tegenwoordig wat minder bekend is,

291
00:15:15,833 --> 00:15:17,433
is Windows Hello for Business.

292
00:15:17,566 --> 00:15:21,133
En je ziet daar vanonder
een screenshot hoe je dat kan instellen.

293
00:15:21,166 --> 00:15:23,900
Dat is een zeer eenvoudige configuratie
voor de eindgebruiker,

294
00:15:23,966 --> 00:15:25,233
IT moet dat activeren.

295

00:15:25,600 --> 00:15:29,266
En dat zorgt ervoor
dat je met een simpele pincode

296
00:15:29,700 --> 00:15:33,200
kan inloggen in je computer
en op die manier toch

297
00:15:33,533 --> 00:15:36,433
via Multi-Factor Authentication
beveiligd bent.

298
00:15:36,500 --> 00:15:40,100
Want die tweede aanmelding
of die tweede manier

299
00:15:40,200 --> 00:15:44,266
om je identiteit te bewijzen
is je toestel zelf.

300
00:15:45,166 --> 00:15:47,233
Dus je gaat met die pincode
en het toestel,

301
00:15:47,300 --> 00:15:49,800
die pincode werkt alleen
op één specifiek toestel,

302
00:15:49,966 --> 00:15:51,233
je identiteit bewijzen.

303
00:15:51,300 --> 00:15:53,833
Op die manier heb je twee zaken,
de pincode en het toestel.

304
00:15:53,900 --> 00:15:55,633
Een beetje vergelijkbaar met je bankkaart

305
00:15:55,700 --> 00:15:58,366
want daar heb je ook
de pincode en de bankkaart.

306
00:15:59,933 --> 00:16:01,000

Ik wil je ook even tonen

307
00:16:01,033 --> 00:16:03,400
hoe die Windows Hello for Business
er concreet uitziet.

308
00:16:03,433 --> 00:16:06,866
Dus dan ga je aanloggen met die pincode
of je kan aanloggen met een paswoord.

309
00:16:06,933 --> 00:16:08,766
Je gaat zien, vanonder heb je twee knoppen

310
00:16:08,833 --> 00:16:12,033
waar je kan switchen
tussen pincode en wachtwoord.

311
00:16:12,100 --> 00:16:14,466
En als die Windows Hello for Business
is ingesteld,

312
00:16:14,566 --> 00:16:16,833
is het gewoon een kwestie
van je pincode in te geven.

313
00:16:16,933 --> 00:16:19,400
Vier cijfers en je bent ingelogd.

314
00:16:19,733 --> 00:16:24,500
Tweede manier hoe je je kan beschermen,
is met een goede wachtwoordmanager.

315
00:16:25,233 --> 00:16:27,433
Wat is dat?
Dat is een soort van digitale kluis

316
00:16:27,533 --> 00:16:29,333
waar je al je wachtwoorden kan insteken

317
00:16:29,533 --> 00:16:32,166
en dan heb je nog één wachtwoord nodig.

318

00:16:32,233 --> 00:16:33,700
Dat mag je uiteraard niet vergeten

319
00:16:33,766 --> 00:16:35,633
want dan heb je natuurlijk
wel een probleem.

320
00:16:36,866 --> 00:16:40,233
Maar zo'n tool laat je dan toe
om naar een website te gaan,

321
00:16:40,266 --> 00:16:42,600
tegen die tool te zeggen:
vul mijn wachtwoord in

322
00:16:43,066 --> 00:16:44,166
en je kan binnen.

323
00:16:44,233 --> 00:16:46,366
Tegenwoordig zit dat ook in de browsers,

324
00:16:46,833 --> 00:16:50,033
maar de mogelijkheden daarvan
zijn eerder beperkt.

325
00:16:51,266 --> 00:16:54,400
Er zijn een paar
bekende, goede wachtwoordmanagers

326
00:16:54,600 --> 00:16:57,800
zoals LastPass, 1Password,
Bitwarden en KeePass

327
00:16:58,266 --> 00:16:59,933
Dat zijn allemaal goede voorbeelden.

328
00:17:00,400 --> 00:17:03,533
De ene is al wat beter dan de andere,

329
00:17:03,633 --> 00:17:05,100
afhankelijk van de functionaliteit

330

00:17:05,133 --> 00:17:10,500
en afhankelijk van hoe goed of slecht ze
de laatste tijd in de media gekomen zijn.

331
00:17:11,133 --> 00:17:13,000
Ook een tip
die ik je nog kan meegeven, is:

332
00:17:13,066 --> 00:17:16,933
gebruik voor elke site
een uniek, voldoende complex paswoord.

333
00:17:17,366 --> 00:17:20,800
Als je dat wil doen, dan heb je
zo'n goede wachtwoordmanager nodig.

334
00:17:20,833 --> 00:17:22,766
Je kan niet al die paswoorden

335
00:17:23,133 --> 00:17:26,433
voor elke site uit het hoofd leren.

336
00:17:27,333 --> 00:17:30,066
Een voorbeeld van zo'n paswoordmanager
is LastPass

337
00:17:30,133 --> 00:17:31,866
en hier hebben we een concreet voorbeeld

338
00:17:31,933 --> 00:17:35,766
waar een aantal logins of notities
in LastPass opgeslagen zijn.

339
00:17:35,833 --> 00:17:39,200
Dus je kan er ook simpele notities maken
zoals de code van je alarm

340
00:17:39,566 --> 00:17:42,233
of de pin- of de pukcodes van gsm's.

341
00:17:42,300 --> 00:17:46,333
Je kan er allerhande informatie insteken.

342
00:17:46,933 --> 00:17:52,100
We hebben daar bijvoorbeeld ook
een login voor Outlook Live in gestoken.

343
00:17:52,233 --> 00:17:55,233
En het leuke is dus,
wanneer je naar die website wil gaan,

344
00:17:55,466 --> 00:17:59,133
dat je niet meer naar die website
handmatig moet gaan en gegevens ingeven

345
00:17:59,166 --> 00:18:01,966
maar je kan rechtstreeks
vanuit LastPass op die site klikken

346
00:18:02,466 --> 00:18:05,733
en dan gaat LastPass
op de site zelf de gegevens ingeven,

347
00:18:05,900 --> 00:18:07,366
komen daar automatisch in terecht.

348
00:18:07,433 --> 00:18:08,900
Je kan vervolgens inloggen

349
00:18:08,966 --> 00:18:14,666
en je zit, zonder dat je een wachtwoord
hebt ingegeven, in het systeem.

350
00:18:14,733 --> 00:18:17,400
Heel erg handig op die manier.

351
00:18:18,033 --> 00:18:20,433
Bovendien is het ook heel erg interessant

352
00:18:20,566 --> 00:18:22,933
om accounts toe te voegen aan LastPass.

353
00:18:23,266 --> 00:18:26,033
Stel, je zit op een website
en je gaat een account aanmaken.

354
00:18:26,333 --> 00:18:29,833
Je moet dan uiteraard eerst
je e-mailadres en je paswoord ingeven,

355
00:18:30,133 --> 00:18:34,466
maar je gaat merken, eens je
die gegevens een voor een ingevuld hebt,

356
00:18:35,166 --> 00:18:38,800
dat LastPass dat zelf gaat detecteren
en gaat zeggen:

357
00:18:38,833 --> 00:18:43,266
Oké, zal ik nu dat wachtwoord
dat je hebt ingegeven opslaan in m'n kluis

358
00:18:43,333 --> 00:18:45,800
zodanig dat je dat later
makkelijker kan raadplegen?

359
00:18:45,833 --> 00:18:48,433
Dat is die melding
die je nu rechtsboven het scherm ziet.

360
00:18:48,633 --> 00:18:50,333
Je kan dan eventueel nog kiezen

361
00:18:50,433 --> 00:18:51,966
om dat in een ander mapje te steken,

362
00:18:52,033 --> 00:18:54,500
om er nog wat extra opties aan te geven.

363
00:18:54,733 --> 00:18:55,800
Je klikt dan op Toevoegen

364
00:18:55,833 --> 00:18:59,000
en vanaf nu zit die account
ook in die kluis.

365
00:18:59,100 --> 00:19:04,033

Dus als je klikt in de browser add-on
ga je zien dat die erbij zit

366
00:19:04,100 --> 00:19:06,700
en als je kijkt in LastPass zelf

367
00:19:06,866 --> 00:19:09,466
zie je dat die accounts
nu toegevoegd zijn.

368
00:19:09,533 --> 00:19:11,366
Als we hier de pagina refreshen,

369
00:19:11,733 --> 00:19:14,266
komen die gegevens ook op het scherm

370
00:19:14,333 --> 00:19:17,133
en dan kan je van hieruit
opnieuw naar de pagina van Coolblue gaan

371
00:19:17,200 --> 00:19:19,966
of kan je de gegevens opvragen

372
00:19:20,266 --> 00:19:23,366
en vanuit die weg
connectie maken met de site.

373
00:19:24,333 --> 00:19:26,466
En dan zijn we bijna rond.

374
00:19:26,933 --> 00:19:32,300
De tip die ik je sowieso nog kan meegeven,
is: gebruik je gezond boerenverstand.

375
00:19:32,766 --> 00:19:34,433
Wordt te weinig verteld,

376
00:19:34,700 --> 00:19:39,033
maar heel vaak kan je al afleiden
uit de sms, uit de mail

377
00:19:39,200 --> 00:19:42,100

of er bijvoorbeeld gehengeld wordt
naar je gegevens,

378
00:19:42,300 --> 00:19:44,233
of je te maken hebt met een phishingmail.

379
00:19:44,933 --> 00:19:47,400
Een goede test daarvoor,
om zelf je kennis eens te testen,

380
00:19:47,433 --> 00:19:50,800
vind je op safeonweb.be,
een website van de overheid

381
00:19:51,133 --> 00:19:54,466
waar je aan de hand van
concrete voorbeelden kan inschatten

382
00:19:54,833 --> 00:19:58,200
of je zo'n phishingmail
al dan niet goed herkent.

383
00:19:58,333 --> 00:20:00,933
Maar een regel die je zeker
in acht mag houden, is:

384
00:20:01,033 --> 00:20:05,933
als het te mooi lijkt om waar te zijn,
is het dat meestal ook.

385
00:20:08,266 --> 00:20:12,233
En uiteraard, maar dat is in mindere mate
voor de eindgebruiker van toepassing,

386
00:20:12,766 --> 00:20:15,233
kan IT ook wel wat inbreng leveren.

387
00:20:15,266 --> 00:20:17,666
Er zijn ook
een aantal IT-gerichte hulpmiddelen.

388
00:20:18,066 --> 00:20:22,266
Zoals: doe zo vaak mogelijk

updates op je toestel.

389
00:20:22,333 --> 00:20:24,766
Updates zijn heel vaak beveiligingsupdates

390
00:20:25,100 --> 00:20:27,900
die de kwetsbare plekken dichtmaken

391
00:20:28,700 --> 00:20:29,733
dus doe dat.

392
00:20:29,833 --> 00:20:32,200
Laat dat niet jaren liggen.

393
00:20:32,566 --> 00:20:36,500
Antivirus, firewall, absoluut noodzakelijk
vandaag op je toestel.

394
00:20:36,833 --> 00:20:41,133
Ook eventueel op je mobiele toestel
kan dat een meerwaarde betekenen.

395
00:20:42,233 --> 00:20:43,633
Dus zonder die dingen

396
00:20:43,833 --> 00:20:47,200
ben je een heel stuk kwetsbaarder
voor al die gevaren.

397
00:20:48,733 --> 00:20:50,800
Tot slot, nog een leuke tip.

398
00:20:51,133 --> 00:20:54,533
Je kan zelf controleren
of je e-mailadres of paswoord

399
00:20:54,633 --> 00:20:57,800
in het illegale circuit
op het internet circuleert,

400
00:20:57,866 --> 00:21:03,166
in een database zit die ooit bijvoorbeeld

ter verkoop is aangeboden op het darkweb.

401
00:21:04,233 --> 00:21:07,500
Die website heet haveibeenpwned.com.

402
00:21:07,633 --> 00:21:08,933
Je kan er gewoon naartoe surfen

403
00:21:09,300 --> 00:21:14,333
en dan kan je, door je e-mailadres
of paswoord in te geven, kijken

404
00:21:14,733 --> 00:21:19,266
of je gegevens ergens
in een gelekte database zitten.

405
00:21:19,333 --> 00:21:21,733
Als dat het geval is,
meteen je paswoord veranderen

406
00:21:21,800 --> 00:21:23,133
en dan ben je terug safe.

407
00:21:23,433 --> 00:21:27,566
Maar daar kan je bijvoorbeeld ook
merken dat het paswoord 123456

408
00:21:27,900 --> 00:21:30,700
een dikke 42 miljoen keer gebruikt is

409
00:21:30,766 --> 00:21:34,200
of in ieder geval
42 miljoen keer in die database zit.

410
00:21:34,266 --> 00:21:35,300
Wel heel leuk

411
00:21:35,366 --> 00:21:39,700
om daar eens te checken
hoe het zit met je persoonlijke gegevens.

412
00:21:39,966 --> 00:21:42,500

Voilà, dat waren
een paar concrete tips en tricks

413
00:21:42,566 --> 00:21:45,966
die ik jullie wou geven
rond cybersecurity.