Draai de digitale deur op slot

MAAK WERK VAN CYBERVEILIGHEID

Als je in de auto stapt, doe je de gordel om. Ga je aan het einde van de werkdag naar huis, dan doe je de deur op slot. Parkeer je je auto, dan laat je je portemonnee niet in de auto liggen. We denken er niet eens meer over na, want het is een automatisme. Helaas is dat voor veel digitale systemen nog niet het geval. Ook die moeten echter op slot. Deze scan helpt je jouw bedrijf digitaal veiliger te maken.

De overheid besteedt veel aandacht aan digitale veiligheid en heeft daarvoor allerlei digitale hulpmiddelen. Een interessante is het Digital Trust Center (www.digitaltrustcenter.nl). Daar zie je in vijf stappen waar je als bedrijf kwetsbaar kunt zijn. Ik neem de proef op de som met een gratis scan. Dat doe ik voor een gemiddeld cumelabedrijf; die telt vijftien medewerkers en heeft de ICT volledig uitbesteed. De eigenaar weet een beetje hoe het zit met de digitale veiligheid van zijn bedrijf. De adviezen in dit artikel zijn het resultaat van deze scan. Ze geven aan wat je als ondernemer kunt doen om het bedrijf beter 'digitaal' op slot te zetten.

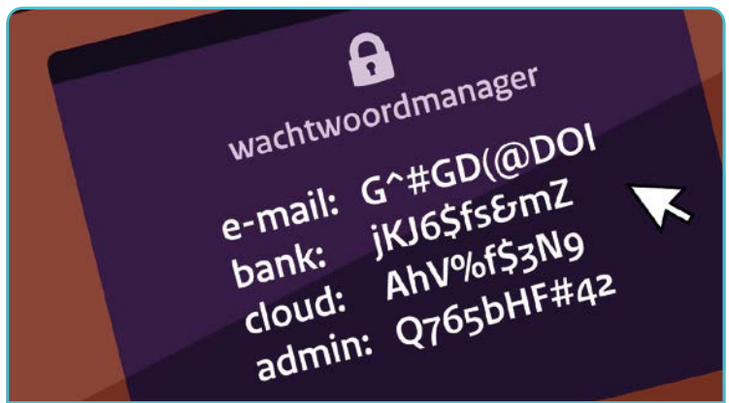
Bij Cumela Verzekeringen vinden we de vragen in de scan praktisch van opzet. Je krijgt daarna een rapportage met goede tips. Het zet je aan het denken. In dit artikel nemen we de basisvragen van de scan, met onze antwoorden, met je door en bespreken we een aantal tips. Maar, let op: elk bedrijf is uniek. Doe daarom in minder dan een half uur de scan voor je eigen bedrijf.

Stap 1. Inventariseer kwetsbaarheden

De vragen en antwoorden bij stap 1 leveren het advies op om een inventarisatie te maken van alle apparatuur en software binnen het bedrijf. Bepaal wat essentieel is voor de bedrijfsvoering,

STAP 1. INVENTARISEER KWETSBAARHEDEN

Vraag	Gegeven antwoord
Ik weet precies welke apparatuur en software er binnen mijn bedrijf wordt gebruikt.	Misschien wel / niet
Ik en mijn medewerkers weten welke gegevens interessant zijn voor kwaadwillenden.	Misschien wel / niet
Ik maak regelmatig een back-up van alle belangrijke informatie.	Misschien wel / niet
Ik weet wie ik moet bellen als er problemen zijn met ICT.	Waarschijnlijk niet
Ik en mijn medewerkers zijn ons bewust van online-dreigingen.	Misschien wel / niet



STAP 2. KIES VEILIGE INSTELLINGEN

Vraag	Gegeven antwoord
Alle standaardwachtwoorden van apparatuur zijn gewijzigd.	Misschien wel / niet
Alle wachtwoorden voor alle apparatuur en software zijn uniek en complex.	Waarschijnlijk niet
Inloggen met gebruikersnaam, veilige wachtwoorden en multifactor-authenticatie.	Waarschijnlijk niet
Met de laptop of mobiele telefoon maken we gebruik van de databundel.	Waarschijnlijk niet
We maken gebruik van een wachtwoordmanager	Zeker niet

STAP 3. UPDATES UITVOEREN

Vraag	Gegeven antwoord
Is alle apparatuur en software voorzien van de laatste updates?	Misschien wel / niet
Wordt er regelmatig gecontroleerd of alles up-to-date is?	Waarschijnlijk niet
Ben jij of de ICT-verantwoordelijke op de hoogte van belangrijke updates?	Waarschijnlijk niet
Staat op alle apparatuur automatisch updaten aan?	Misschien wel / niet
Iedereen installeert updates direct.	Waarschijnlijk niet

STAP 4. TOEGANG BEPERKEN TOT DATA EN OF TOEPASSINGEN

Vraag	Gegeven antwoord
Is er beleid voor een eigen gebruikers naam uniek wachtwoord?	Zeker niet
Iedereen kan alleen bij de informatie die hij nodig heeft voor zijn werkzaamheden.	Misschien wel / niet
Als een medewerker uit dienst gaat, levert hij direct alle bedrijfsmiddelen in.	Misschien wel / niet
Als een medewerker uit dienst gaat, wordt direct de toegang tot alles afgesloten.	Misschien wel / niet
Mijn bedrijfsnetwerk is alleen toegankelijk voor mij en mijn medewerkers/collega's.	Waarschijnlijk niet

zoals planning, personeels- en klantenadministratie, en apparaten zoals laptops, weegbruggen en telefoons. Bepaal wat je echt moet beschermen en werk samen met je ICT-dienstverlener om een noodplan op te stellen. Dat plan beschrijft hoe je dit gaat doen en hoe je alles na een cyberincident weer aan de gang kunt krijgen. Zet dit noodplan op papier en bewaar het veilig. Bespreek en oefen het plan regelmatig met een deskundige, zoals je ICT-dienstverlener. Oefen bijvoorbeeld halfjaarlijks met het terugplaatsen van de back-up. Een papieren bellijst van IT-dienstverleners en medewerkers is handig om snel hulp te kunnen inroepen bij een cyberincident. Zo voorkom je paniek tijdens een aanval en bespaar je tijd.

Stap 2. Kies veilige instellingen

Het advies bij stap 2: Maak voor alle software en apparatuur unieke en complexe wachtwoorden en sla deze op in een wachtwoordmanager. Probeer ook andere vormen voor het maken van een wachtwoord. Gemakkelijker te onthouden en tegelijk moeilijker te kraken zijn wachtwoordzinnen, bijvoorbeeld 'Cumela is 1 betrouwbare organisatie!'. Nog veiliger is het gebruik van multifactor-authen-

STAP 5. VIRUSSEN EN ANDERE BEDREIGINGEN VOORKOMEN

Vraag	Gegeven antwoord
Iedereen is in staat om verdachte e-mails en links te herkennen.	Waarschijnlijk niet
Alle apparatuur heeft antivirussoftware en is up-to-date.	Misschien wel / niet
Software downloaden kan pas na toestemming.	Misschien wel / niet
Iedereen meldt het als hij denkt slachtoffer te zijn van een virus of kwade software.	Misschien wel / niet

ticatie dan voeg je bij het inloggen ook nog een code in die je op je telefoon ontvangt. Dan is hacken nagenoeg onmogelijk.

Stap 3. Updates uitvoeren
Updaten is cruciaal voor alle met het netwerk en of internet verbonden apparaten, zoals je computer, printer, camerasysteem, weegbrug, toegangshek of router. Dit is belangrijk omdat softwareleveranciers continu bezig zijn om hun producten beter te beschermen tegen hackers. Is er een update? Niet wachten, gelijk installeren. Doe je dit niet? Dan ben je kwetsbaar. Automatisch updaten instellen voorkomt dat je hierin veel tijd moet investeren. Kan automatisch updaten niet? Zet dan in je agenda dat je dit maandelijks handmatig doet.

Stap 4. Toegang beperken tot data en of toepassingen
Het advies van stap 4: Geef de financieel eindverantwoordelijke alleen toegang tot je bankgegevens als hij ook de betalingen doet. Trek die rechten in als een medewerker uit dienst gaat. Als ondernemer is het juist wel belangrijk om uitgebreide toegangsrechten te hebben, zodat je altijd overal bij kunt. Het is ook belangrijk om een tweede persoon die rechten te geven voor noodsituaties.

Stap 5. Virussen en andere bedreigingen voorkomen
Een virus verstoort systemen of verzamelt of versleutelt informatie. Het kan binnenkomen via geïnfecteerde e-mails, bezochte websites of besmette usb-sticks. Criminelen gebruiken deze methoden om je systeem over te nemen of gegevens te stelen. Vaak wordt dit gevolgd door afpersing, namelijk dat je de gegevens pas terugkrijgt als je losgeld betaalt. Train jezelf en je medewerkers om risico's te herkennen met de filmpjes op Samen Digitaal Veilig.

WEBINAR NIS2: CYBERBEVEILIGINGSWET

Ben jij steeds afhankelijker van automatisering en ICT? Wil je weten hoe je dit goed en veilig kan oplossen? Volg dan ons webinar op donderdag 26 september vanaf 15.00 uur. Je hoort tips uit de praktijk van Jolanda Hogendoorn (Arie Hogendoorn Grondverzet) en krijg praktische handvaten om digitaal veilig te werken van een expert. Hij deelt ook informatie over de nieuwe wet NIS2.

Er zijn geen kosten verbonden aan jouw deelname. Meld je aan via www.cumela.nl/webinardigitaalslagvaardig

WAT IS NIS2?
Een Europese richtlijn voor netwerk- en informatiebeveiliging. Deze legt strengere cybersecuritymaatregelen op aan bedrijven of organisaties in essentiële en belangrijke sectoren, zoals waterschappen. In Nederland noemen we dit de Cyberbeveiligingswet. Veel bedrijven in onze sector doen werkzaamheden voor deze bedrijven of organisaties uit en kunnen er dus mee te maken kunnen krijgen. Cumela leverde via VNO-NCW en MKB Nederland input voor de internetconsultatie van het Nederlandse wetsvoorstel. Wij vinden dat de eisen aan onze sector beperkt moeten blijven. Ons type bedrijven hoor je niet op te zadelen grote extra administratieve lasten.

SAMEN DIGITAAL VEILIG

Je kunt naast de basisscan van het Digital Trust Center ook meedoen aan Samen Digitaal Veilig. Dan krijg je ook de beschikking over handige checklists, video's en actuele informatie. Deelname aan de basisversie van Samen Digitaal Veilig is ook kosteloos en helpt je om jouw digitale basisveiligheid te vergroten. Via www.cumela.nl/nieuws/samen-digitaal-veilig kun je je registreren, zodat je kosteloos kunt deelnemen aan Samen Digitaal Veilig.

Verder zijn er nog een aantal hulpmiddelen die je kunt gebruiken:

Meterkastkaart:	www.digitaltrustcenter.nl/sites/default/files/2023-05/Bellijst.pdf
Vijf basisprincipes:	www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen
Fraude-quiz:	www.digitaltrustcenter.nl/test-je-kennis/fraude
Herken phishing-quiz:	www.digitaltrustcenter.nl/test-je-kennis-phishing
Zeven tips:	www.digitaltrustcenter.nl/sites/default/files/2023-05/checklist_starten_met_cybersecurity.png

JE FIETS OP SLOT ZETTEN
Door zelf de scan van het Digital Trust Center in te vullen, krijg je inzicht in de digitale weerbaarheid van jouw bedrijf. De antwoorden kunnen je helpen om gericht aan de slag te gaan met de digitale veiligheid. Door aandacht te besteden aan de praktische tips uit het rapport, zoals goede en unieke wachtwoorden (of beter nog wachtwoordzinnen), multifactor-authenticatie en automatisch updaten, wordt jouw digitale veiligheid al net zo logisch als je fiets op slot te zetten. Blijf zelf, samen met jouw medewerkers en ICT-dienstverlener, werken aan jouw digitale veiligheid.

Tekst: Gerwin Otten, adviseur preventie Cumela Verzekeringen