Cyberweerbaarheid Scan | Vragenlijst

Neem ter voorbereiding op de Cyberweerbaarheid Scan de volgende vragen door. De vragen hebben betrekking op alle digitale aspecten van je organisatie, de techniek, het onderhoud, de huisvesting, de privacy en de continuïteit. Beantwoord de vragen samen met iemand die verantwoordelijk is voor de ICT, zodat je deze tijdens de Scan gemakkelijk kunt beantwoorden.

Vragenlijst

Nr.	Categorie	Vraag
1	Organisatie	Heeft uw organisatie richtlijnen opgesteld voor informatieveiligheid en privacybescherming?
2	Organisatie	Heeft uw organisatie de medewerkers geïnformeerd over hun verantwoordelijkheden op het gebied van privacy en informatiebeveiliging?
3	Organisatie	Verzorgd uw organisatie trainingen om medewerkers en externen bewust te maken van Cyberrisico's?
4	Organisatie	Stimuleert uw organisatie medewerkers in het melden van cybersecurity incidenten?
5	Organisatie	Heeft uw organisatie afspraken gemaakt met medewerkers, over het zelf vergrendelen van hun systeem als ze van hun werkplek weglopen?
6	Organisatie	Maakt uw organisatie uitsluitend gebruik van Cloudapplicaties?
7	Organisatie	Is het (Wi-Fi) netwerk van uw organisatie alleen toegankelijk medewerkers en contractanten?
8	Organisatie	Heeft uw organisatie een separaat en geïsoleerd Wi-Fi gastennetwerk?
9	Organisatie	Heeft uw organisatie bij in- en uitdiensttreding van medewerkers het tijdig aanmaken, wijzigen of intrekken van gebruikerstoegang goed op orde?
10	Organisatie	Heeft u formele verwerkersovereenkomsten afgesloten voor het delen van gegevens en data met leveranciers en partners die voor uw organisatie gegevens verzamelen, genereren, verwerken en/of opslaan?
11	Organisatie	Laat u de ICT-infrastructuur van uw organisatie wel eens beoordelen door externe deskundigen?
12	Organisatie	Heeft uw organisatie een vast contactpersoon aangewezen voor het melden van verdachte situaties?
13	Organisatie	Heeft uw organisatie inzichtelijk wie binnen uw ICT-infrastructuur over 'administrator' rechten beschikt?
14	Organisatie	Zorgt u ervoor dat 'oude' hardware veilig wordt verwijderd? (wissen data, harde schijven vernietigen)
15	Organisatie	Dwingt uw organisatie af dat alle vormen van bestandsoverdracht (mail, USB-sticks, File sharing, et cetera) veilig moeten verlopen?
16	Organisatie	Heeft uw organisatie, met betrekking tot de organisatie van informatiebeveiliging, duidelijke afspraken vastgelegd met ICT-toeleveranciers?
17	Techniek	Maakt u gebruik van Microsoft365, of vergelijkbare producten, zoals Google Workspace of Amazon Workspace?
18	Techniek	Heeft uw organisatie Multi Factor Authenticatie ingericht?
19	Techniek	Worden dagelijks gedeeltelijke/volledige back-ups gemaakt?

20	Techniek	Wordt er minimaal wekelijks één niet-overschrijfbare Offline back-up gemaakt en bewaard op een andere locatie, zodat deze niet onklaar kan worden gemaakt?
21	Techniek	Maakt u gebruik van een Spamfilter voor inkomend email verkeer?
22	Techniek	Heeft uw organisatie versleutelingsmaatregelen (Encryptie) genomen om informatie/data, te beschermen tegen onbevoegde inzage en wijziging, zowel tijdens opslag als transport van de gegevens?
23	Techniek	Zijn er in geval van ICT-uitbesteding over het thema Techniek contractuele afspraken gemaakt met de ICT-leverancier van uw organisatie?
24	Onderhoud	Worden de applicaties en besturingssystemen die binnen uw organisatie worden gebruikt regelmatig voorzien van updates?
25	Onderhoud	Zorgt uw organisatie ervoor dat de Firewall(s) correct zijn geconfigureerd en gebruik maken van de nieuwste software/firmware?
26	Onderhoud	Heeft uw organisatie Firewall en netwerkbeveiliging ingeschakeld op alle pc's en laptops?
27	Onderhoud	Heeft uw organisatie virus- en bedreigingsbeveiliging ingeschakeld op alle pc's en laptops?
28	Onderhoud	Heeft uw organisatie virus- en bedreigingsbeveiliging ingeschakeld op alle servers of hosts?
29	Onderhoud	Heeft uw organisatie het wifi netwerk adequaat beveiligd met Wi-Fi Protected Access (encryptie)?
30	Onderhoud	Heeft uw organisatie het Wi-Fi netwerk adequaat beveiligd een moeilijk toegangswachtwoord?
31	Onderhoud	Heeft uw organisatie ervoor gezorgd dat niet iedereen het Wi-Fi apparaat kan detecteren door het SSID-signaal (Service Set IDentifier) uit te schakelen?
32	Onderhoud	Heeft uw organisatie inzichtelijk wat medewerkers mogen en kunnen binnen het netwerk en systemen?
33	Onderhoud	Geeft uw organisatie medewerkers alleen die toegang en rechten, die ze voor hun werk nodig hebben?
34	Onderhoud	Heeft uw organisatie, van alle apparaten die binnen de Infrastructuur vallen de fabriekswachtwoorden gewijzigd naar een nieuw en moeilijk te raden toegangswachtwoord/zin
35	Onderhoud	Voldoen de wachtwoorden die uw organisatie hanteert minimaal aan de volgende eisen? • Het wachtwoord bestaat uit (minimaal) 10 tekens, waarbij minimaal 1 numeriek teken en minimaal 1 leesteken wordt gebruikt. • Het wachtwoord is 60 dagen geldig en dient daarna vervangen te worden door een nieuw wachtwoord. • Het wachtwoord kan slechts éénmaal gebruikt worden. • Gebruikersaccounts en wachtwoord zijn persoonlijk en nooit overdraagbaar.

36	Onderhoud	Vervangt u apparaten of software als updates van leveranciers niet meer beschikbaar zijn, of ondersteund worden.
37	Onderhoud	Zorgt uw organisatie ervoor dat systemen (computer, laptop, telefoons) automatisch na een aantal minuten vergrendelen (locken), zodat deze niet toegankelijk zijn voor onbevoegden?
38	Onderhoud	Heeft iedere medewerker een eigen gebruikersaccount, dus geen gedeelde accounts?
39	Onderhoud	Zijn er in geval van ICT-uitbesteding over het thema onderhoud contractuele afspraken gemaakt met de ICT-leverancier(s) van uw organisatie?
40	Huisvesting	Is uw kantoor beveiligd tegen onbevoegde fysieke toegang?
41	Huisvesting	Kunnen mensen van buiten het kantoor naar binnen kijken en zo op uw beeldschermen kijken?
42	Huisvesting	Zijn uw serveromgeving en netwerkcomponenten (zoals routers en switches) beveiligd tegen onbevoegde fysieke toegang?
43	Huisvesting	Hanteert u 'Clean Desk' richtlijnen
44	Privacy	Heeft uw organisatie technische en organisatorische maatregelen getroffen voor het tijdig kunnen verwijderen van gegevens die de limiet van hun bewaartermijn hebben bereikt?
45	Privacy	Wordt uw bedrijfs- en klantdata zoveel mogelijk verwerkt en opgeslagen binnen de EU?
46	Privacy	Houdt uw organisatie een verwerkingsregister bij in verband met de documentatie- en verantwoordingsplicht die geldt bij het verwerken van persoonsgegevens?
47	Privacy	Verwerkt u alleen de persoonsgegevens die u daadwerkelijk nodig heeft om aan uw wettelijke verplichtingen te voldoen?
48	Continuïteit	Heeft uw organisatie een draaiboek voor Datalekken?
49	Continuïteit	Heeft uw organisatie een draaiboek Ransomware?
50	Continuïteit	Heeft uw organisatie een inventarisatie gemaakt van alle computers, software, clouddiensten, slimme apparaten etc., voorzien van bijbehorende software-versies en serienummers?
51	Continuïteit	Test uw organisatie het terugzetten van de back-ups en indien van toepassing een Server snapshot, waarbij een controle op inhoud, volledigheid en correctheid plaatsvindt?