Checklist Risicobeoordeling– Cybersecurity

Geweldig dat u heeft besloten om deze gratis Checklist Risicobeoordeling te downloaden en dat u aan de slag gaat met het beschermen van uw organisatie.

Het is essentieel dat u niet alleen weet waar uw organisatie staat, maar ook wat de belangrijkste aandachtspunten zijn om uw systemen, data en processen te beschermen.

De **Checklist Risicobeoordeling** van TechSolv geeft u snel en duidelijk inzicht in de huidige staat van uw cybersecurity. Door eerlijk en grondig te antwoorden krijgt u een helder beeld waar uw organisatie sterke en zwakke punten heeft en welke gebieden de hoogste prioriteit verdienen.

Met deze uitgebreide beoordeling kunt u gericht investeren in de juiste beveiligingsmaatregelen, compliance bereiken en uw organisatie weerbaar maken tegen de steeds evoluerende cyberdreigingen.

Hoe gebruikt u deze Checklist Risicobeoordeling?

1. **Neem de tijd en wees eerlijk:**
   Beantwoord elke vraag door de schaal van 1 (zeer laag risico) tot 5 (hoog risico) toe te wijzen op basis van de situatie binnen uw organisatie. Wees realistisch; de waarde ligt in een betrouwbare beoordeling.

2. **Ga systematisch te werk:**
   Door elke sectie rustig door te nemen, krijgt u een compleet beeld. Noteer uw antwoorden en tel de cijfers aan het einde op. Doe dit alleen of met collega's, de discussie over dit onderwerp is goed.

3. **Bepaal uw risicogebieden:**
   De punten geven aan waar de meeste risico's liggen. Focus op de gebieden met de hoogste scores voor actie en verbetering.

4. **Gebruik de score voor prioriteitstelling:**
   Hoe hoger de uiteindelijk score, hoe groter de risico's en de urgentie om maatregelen te nemen.

5. **Plan vervolgstappen:**
   Op basis van uw score is het verstandig om een specialist zoals TechSolv te raadplegen voor gerichte adviezen en ondersteuning. Op de website van TechSolv kunt u een gratis advies gesprek plannen. Zonder verplichtingen achteraf.
   Vragen?
   Heeft u vragen over het gebruik van deze checklist, stel deze dan gerust per e-mail op hallo@techsolv.nl we helpen u snel!

1. Infrastructuur en Netwerken

- Zijn firewalls en netwerksegmentatie geïmplementeerd en up-to-date?
- Worden netwerktoegangen en -verkeer voortdurend bewaakt?
- Is uw Wi-Fi beveiligd met WPA2/WPA3 en hebt u gescheiden netwerken voor gasten en medewerkers?
- Zijn verbindingen via VPN veilig en goed geconfigureerd?
- Worden kwetsbaarheden in netwerkapparatuur regelmatig gescand en geüpdatet?

Risiconiveau (1-5): _ _ _ _

---

2. Systemen en Applicaties

- Worden alle systemen en software up-to-date gehouden met de laatste beveiligingspatches?
- Is er een beleid voor het beheer van software en applicaties?
- Worden wijzigingen en configuraties in systemen zorgvuldig gedocumenteerd?
- Heeft u werkplek beveiliging (antivirus, anti-malware) op al uw apparaten?
- Zijn uw systemen beschermd tegen bekende exploits en kwetsbaarheden?

Risiconiveau (1-5): _ _ _ _

---

3. Data en Data Beveiliging

- Is gevoelige data versleuteld, zowel in rust als tijdens verzending?
- Worden back-ups regelmatig gemaakt en getest?
- Zijn toegangsrechten tot data strikt beheerd en geïmplementeerd op basis van ‘least privilege’?
- Is er logging en monitoring van toegangs- en datatransacties?
- Worden data- en privacyregels nageleefd (bijvoorbeeld GDPR)?

Risiconiveau (1-5): _ _ _ _

---

4. Gebruikers en Toegangsbeheer

- Heeft u een wachtwoordbeleid met complexe wachtwoorden en regelmatige verversing?
- Wordt multi-factor authenticatie (MFA) toegepast voor toegang tot kritieke systemen?
- Zijn gebruikersrechten en toegangsrechten regelmatig herzien?
- Worden authenticatie- en toegangsactiviteiten gelogd en gecontroleerd?
- Worden medewerkers getraind in veilig gebruik van wachtwoorden en het herkennen van phishing?

Risiconiveau (1-5): _____

---

5. Security Awareness en Training

- Heeft u periodieke security awareness trainingen voor alle medewerkers?
- Worden medewerkers getest op het herkennen van phishing en andere aanvallen?
- Zijn er procedures voor veilig omgaan met e-mails en bijlagen?
- Worden medewerkers bewust gemaakt van social engineering technieken?
- Is er een cultuur van security en openheid over incidenten?

Risiconiveau (1-5): _____

---

6. Incident Response en Monitoring

- Is er een vastgesteld incident response plan en worden medewerkers hierin getraind?
- Wordt er continue gemonitord op verdachte activiteiten en dreigingen?
- Zijn er tools zoals SIEM of intrusion detection systems geïmplementeerd?
- Kan uw organisatie snel reageren op incidenten en datalekken?
- Worden incidenten gedocumenteerd en geëvalueerd om herhaling te voorkomen?

Risiconiveau (1-5): _____

7. Organisatie en Beleid

- Heeft u formeel vastgelegde security- en privacybeleid?
- Zijn alle medewerkers op de hoogte van hun verantwoordelijkheid?
- Worden procedures voor databeveiliging en incidenten nageleefd en geëvalueerd?
- Heeft u een aangewezen security verantwoordelijke of CISO?
- Worden bewaarplichten en privacyvereisten strikt nageleefd?

Risiconiveau (1-5): _____

---

8. Regelgeving en Certificeringen

- Bent u compliant met GDPR en andere relevante regelgeving?
- Heeft u relevante certificeringen (ISO27001, NIST, etc.)?
- Worden audits en assessments regelmatig uitgevoerd?
- Is er een lange termijn security-roadmap?
- Worden compliance- en security-vereisten expliciet meegenomen in contracten met leveranciers en partners?

Risiconiveau (1-5): _____

---

9. Eindscore en Prioriteiten

Tel alle ingevulde scores bij elkaar op voor een totaal.
De maximale score per item is 5, en er zijn 8 items, dus de maximale totaalscore is 40.

Score interpretatie:

- ** totaal 8-15 punten:** *Laag risico*
  Uw organisatie heeft goede maatregelen op orde, maar er blijven aandachtspunten. Voer periodieke updates door en blijf alert.
- **Score 16-25 punten:** *Gemiddeld risico*
  Uw organisatie heeft een degelijke basis, maar er is ruimte voor verbetering. Prioriteer zwakke plekken zoals patchmanagement, gebruikersbewustzijn of monitoring.
- **Score 26-40 punten:** *Hoog risico*
  Uw organisatie is kwetsbaar voor cyberaanvallen en datalekken. Neem snel actie op de punten die de hoogste risico's aangeven. Overweeg een uitgebreide security audit en professionele ondersteuning.

10. Aanbevolen Vervolgstappen

Bij TechSolv geloven we dat inzicht pas de eerste stap is. Om echt resultaat te boeken en uw organisatie optimaal te beveiligen, is het belangrijk om verder te kijken dan alleen de score.

Wij adviseren u:

- Gebruik de uitkomst van deze checklist om risico's en prioriteiten concreet te maken.
- Plan een vrijblijvend en gratis adviesgesprek met onze security experts via onze website **techsolv.nl**.
- Tijdens dit gesprek bespreken we uw resultaten, geven we praktische aanbevelingen en helpen we u een effectief beveiligingsplan op te zetten — zonder enige verplichtingen.

Wacht niet langer!
Beveilig uw organisatie proactief en voorkom dat u het slachtoffer wordt van een cyberincident.

Deze checklist helpt je inzicht te krijgen, maar echte security is een doorlopend proces.
Blijf alert, blijf verbeteren!