Uw digitale risico's

Vragenlijst

Deze vragenlijst ondersteunt u om de interne en externe factoren te herkennen die van invloed zijn op uw digitale risico's. Hierdoor krijgt u een beter overzicht van relevante digitale risico's bij het ontwikkelen van interne controle- en beheersingsmaatregelen.

Kiest u per vraag het antwoord dat het beste bij uw situatie past. Bij sommige vragen zijn meerdere antwoorden mogelijk, dit staat bij de betreffende vragen aangegeven.

1. Algemeen

1. Met welk doel gebruikt uw bedrijf technologie?
- o Ons bedrijf gebruikt computersystemen voor het ondersteunen van interne, ondersteunende afdelingen.
- o De computersystemen ondersteunen onze primaire bedrijfsprocessen.
- o Er worden computersystemen gebruikt voor het produceren/assembleren van producten.
- o Computersystemen ondersteunen de dienstverlening aan onze klanten.
- o E-commerce/online verkoop.
- o Geen van bovenstaande.

2. Welke persoonsgegevens van klanten, werknemers en/of anderen bewaart uw onderneming?
- o Persoonlijke gegevens (NAW-gegevens, etc.).
- o Financiële gegevens (creditcards, etc.).
- o Gezondheidsgegevens (medische dossiers, etc.).
- o Overige privégegevens (BSN, levensovertuiging, vakbondslidmaatschap, religie, etc.).
- o Er worden geen persoonsgegevens bewaard.

3. Hoe worden uw management en directie geïnformeerd over digitale risico's?
- o Digitale risico's worden via de reguliere bedrijfsvoering geadresseerd.
- o Via een speciaal beveiligingsteam dat regelmatig bijeenkomt en over haar activiteiten rapporteert aan ons senior management.
- o Onze directie wordt regelmatig geïnformeerd, er zijn beveiligingsupdates en bijeenkomsten voor belanghebbenden met een constante monitoring van het geheel aan digitale risico's en daaraan gerelateerde incidenten.
- o Geen van bovenstaande.

2. ICT-infrastructuur en hardware

4. Hoe wordt er binnen uw bedrijf voor gezorgd dat er op de juiste manier aandacht wordt gegeven aan de ICT-beveiliging?
(meerdere antwoorden mogelijk)
- o Ons hoofd ICT-beveiliging (of equivalent) en zijn team worden nauw betrokken en werken samen met de rest van ons bedrijf.
- o Ons hoofd ICT-beveiliging (of equivalent) rapporteert rechtstreeks aan het management (de directie) van ons bedrijf.
- o Er wordt op alle technische gebieden gewerkt met ICT-beveiligingsrichtlijnen.
- o Onze werknemers worden betrokken bij beveiliging van ICT-systemen en gegevens. Zij zijn zich bewust van hun verantwoordelijkheid op dit gebied.
- o Er worden periodiek (externe) audits uitgevoerd van de ICT-toepassingen en infrastructuurbeheersmiddelen binnen het bedrijf.
- o Geen van bovenstaande.

5. Hoe controleert uw bedrijf de toegang tot uw ICT-systemen?
- o Via multifactor-authenticatie (het bewijzen van een identiteit door de combinatie van verschillende factoren, zoals pinnen met uw pinpas én pincode).
- o Er is een wachtwoord nodig voor toegang tot al onze bedrijfskritische toepassingen.
- o Er is een wachtwoord nodig voor toegang tot al onze bedrijfskritische toepassingen, maar er kan één wachtwoord worden gebruikt voor meerdere applicaties (Single Sign-On).
- o Anders, namelijk _____
- o Geen van bovenstaande.

Postbus 8789, 3009 AT Rotterdam ▶ 010 - 288 44 44 ▶ www.schoutenzekerheid.nl

Vragenlijst

6. Is er sprake van een consistente versleuteling van uw gevoelige/ kritieke data? *(meerdere antwoorden mogelijk)*
- o Ja, alle data op onze mobiele apparaten is versleuteld.
- o Ja, alle data die geclassificeerd is als gevoelig, is versleuteld in rusttoestand.
- o Ja, alle data die geclassificeerd is als gevoelig, is versleuteld tijdens 'transit'.
- o Ons bedrijf heeft geen consistent beleid, onze versleuteling is nog in ontwikkeling.
- o Nee.

7. Heeft u het internetverkeer op uw website versleuteld (bijvoorbeeld door middel van HTTPS of SSL) voor een veilige gegevensoverdracht?
- o Ja.
- o Nee.

8. Kunnen medewerkers door middel van usb-sticks data van het netwerk halen / op het netwerk zetten?
- o Ja.
- o Nee.

9. Mogen werknemers hun eigen smartphones, tablets en laptops gebruiken voor toegang tot beschermde bedrijfsgegevens en applicaties (BYOD: 'Bring Your Own Device')?
- o Ja, en er bestaat een streng beveiligings-/ versleutelingsbeleid.
- o Ja, maar er bestaat geen streng beveiligings-/ versleutelingsbeleid.
- o Ja, maar ik weet niet of er sprake is van een beveiligings-/ versleutelingsbeleid.
- o Nee.

10. Welke andere mogelijkheden voor mobiel ICT-gebruik biedt uw organisatie aan werknemers?
- o Apparaten kunnen via draadloze netwerken (wifi) verbinding maken met onze bedrijfssystemen.
- o Ons bedrijf stelt werknemers in staat om op afstand toegang te krijgen tot bedrijfssystemen (bijvoorbeeld bij thuiswerken).
- o Anders, namelijk _____
- o Geen van bovenstaande.

11. Gebruikt u clouddiensten?
- o Ja, voor het opslaan van privé- en/of vertrouwelijke bedrijfsgegevens.
- o Ja, alleen voor het opslaan van algemene en algemeen toegankelijke informatie.
- o Nee.

12. Hoe zorgt uw bedrijf ervoor dat gegevens op back-uptapes ontoegankelijk zijn voor onbevoegde personen? *(meerdere antwoorden mogelijk)*
- o Onze back-uptapes zijn versleuteld.
- o Onze back-uptapes worden opgeborgen in een gesloten vuurbestendige locatie.
- o Onze back-uptapes worden buiten kantoor bewaard op een veilige locatie.
- o Anders, namelijk _____
- o Wij maken geen back-ups.

3. ICT-applicaties en software

13. Zijn de toegangsrechten van alle gebruikers gebaseerd op hun individuele functieprofiel en verantwoordelijkheden?
- o Ja.
- o Nee.

14. Bestaan er strenge autorisatievereisten voor werknemers die applicaties willen downloaden/installeren op hun werkcomputers?
- o Ja.
- o Nee.

15. Hoelang denkt u dat kritische applicaties en systemen kunnen zijn uitgeschakeld (buiten werking) voordat uw bedrijf er aanzienlijke schade van ondervindt?
- o 0 - 1 uur.
- o 1 - 6 uur.
- o 6 uur - 1 dag.
- o Langer dan 1 dag.

16. Bestaat er een formele procedure voor het beheren en configureren van de kritische toepassingen en systemen, firewalls, antivirussoftware, spamfilters en antimalware?
- o Ja.
- o Ja, en updates worden centraal geregeld en uitgevoerd.
- o Nee.

4. Toezicht op gegevensbescherming

17. Hoe wordt er binnen uw bedrijf voor gezorgd dat gegevens beschermd zijn? *(meerdere antwoorden mogelijk)*
- o Binnen ons bedrijf is duidelijk wie er verantwoordelijk is voor de gegevensbescherming.
- o Het hoofd gegevensbescherming heeft een gegevensbeveiligingsstrategie en rapporteert aan het passende managementniveau binnen ons bedrijf over de naleving van die strategie.
- o Werknemers krijgen geregeld training op het gebied van gegevensbescherming passend bij hun functie, en zijn betrokken en zich bewust van de eigen verantwoordelijkheden ten aanzien van het beschermen van (persoons)gegevens.
- o In de afgelopen twee jaar heeft er een audit plaatsgevonden van het naleven van de gegevensbeschermingswetgeving door ons bedrijf.
- o Geen van bovenstaande.

Postbus 8789, 3009 AT Rotterdam 010 - 288 44 44 www.schoutenzekerheid.nl

18. Hoe wordt er binnen uw bedrijf voor gezorgd dat normen op het gebied van gegevensbescherming nageleefd worden? *(meerdere antwoorden mogelijk)*
- o Er bestaat een gegevensbeschermingsbeleid.
- o Het gegevensbeschermingsbeleid en de gegevensbeschermingsprocedures worden uitgevoerd middels regelmatige zelfcertificeringen, personeelsberichten en intranet, werknemershandboeken en periodieke compliance audits.
- o De gegevensbeheerder wordt met name betrokken bij belangrijke veranderingen in het bedrijf (bijvoorbeeld overnames, klantovereenkomsten, overeenkomsten met nieuwe leveranciers).
- o Ons bestuur vraagt periodiek om updates over belangrijke onderwerpen op het gebied van gegevensbescherming.
- o Geen van bovenstaande.

19. Hoeveel persoonsgegevens (ook wel: records) slaat uw bedrijf gemiddeld op? Houdt bij uw inschatting rekening met werknemers, informatie, klant- en leveranciersgegevens, etc.
- o Minder dan 250.000 records.
- o 250.000 tot 500.000 records.
- o 500.000 tot 1.000.000 records.
- o tot 5.000.000 records.
- o Meer dan 5.000.000 records.

20. Houdt een zakelijke partner of leverancier persoonlijke gegevens bij namens u, of levert deze aan u ICT-diensten (supply chain risico)? *(meerdere antwoorden mogelijk)*
- o Ja, we vereisen daarom bewijs dat een derde partij het ICT-risico heeft beoordeeld.
- o Ja, zij stellen een limiet aan de verantwoordelijkheid betreffende de diensten die zij leveren.
- o Ja, zij sluiten alle relevante verzekeringspolissen af voor fouten en nalatigheden.
- o Nee.

21. Is uw onderneming actief in verschillende jurisdicties (rechtsgebieden)?
- o Ja.
- o Ja, waaronder de Verenigde Staten (USA).
- o Nee.

22. Hoe bereidt u zich voor op (aanstaande) wet- en regelgeving op het gebied van informatiebeveiliging en privacy?
- o Wij houden het in de gaten en we hebben een projectplan.
- o Wij houden het in de gaten en relevante besluiten worden pas gemaakt wanneer de uiteindelijke richtlijn van kracht wordt.
- o Wij houden ons er niet in het bijzonder mee bezig.

5. Cyberaanvallen, systeemstoringen en inbreuken op gegevensbeveiliging

23. Is er binnen uw bedrijf een overkoepelend (risicomanagement) programma voor het tegengaan van kwetsbaarheden in uw ICT-systemen?
- o Ja, systemen ter voorkoming (preventie) en detectie van inbreuken.
- o Ja, we testen periodiek op het binnendringen en misbruik van ICT-systemen.
- o Ja, middels het gebruik van een Security Information & Event Management methodiek (SIEM).
- o Geen van bovenstaande.

24. Bent u in de afgelopen 12 maanden het slachtoffer geweest van inbreuken op uw netwerk, verlies of diefstal van gegevens, of omvangrijke systeemstoringen (al dan niet als gevolg van kwaadaardige activiteiten)?
- o Ja, met gevolgen voor het bedrijf.
- o Ja, zonder gevolgen voor het bedrijf.
- o Nee.

25. Heeft uw organisatie een actieplan voor cyberincidenten en een multidisciplinair team dat in geval van een crisissituatie in actie komt?
- o Ja, en het is duidelijk gedocumenteerd. Bovendien wordt het plan minimaal één keer per jaar getest met simulaties, en worden verbeteringen op continue basis in het plan bijgewerkt.
- o Ja, er geldt een meldingsplicht voor iedereen om een (vermoedelijk) beveiligingsincident te melden.
- o Ja, maar het is niet gedocumenteerd.
- o Nee.

Postbus 8789, 3009 AT Rotterdam 010 - 288 44 44 www.schoutenzekerheid.nl