IT security manager

Informatiebrochure

Breng je IT-beveiliging op orde

IT security manager: vertrouw altijd op een goede beveiliging

Gestolen informatie en gegijzelde systemen zijn tegenwoordig aan de orde van de dag. Niet vreemd als je bedenkt dat bedrijven steeds afhankelijker zijn van IT-systemen, maar weinig tijd en geld investeren in de beveiliging van die systemen. Momenteel is de kans dat jouw bedrijf slachtoffer wordt van een cyberaanval 1 op 8. Bizar hoog, helemaal als je bedenkt dat de kans op een brand 1 op 8000 is.

Maar hoe voorkom je dat jouw bedrijf te maken krijgt met cybercriminelen? Simpel: door te zorgen voor een goede IT-beveiliging houd jij de luiken gesloten en probeert de hacker het bij de buren. Met onze IT security manager helpen wij het mkb met het op orde krijgen en houden van de beveiliging. We geven tips, advies en controleren periodiek of de beveiliging nog standhoudt tegen criminelen. Zo kun jij vertrouwen op een goede IT-beveiliging.

INHOUDSOPGAVE

1. Beveiliging op orde krijgen en houden

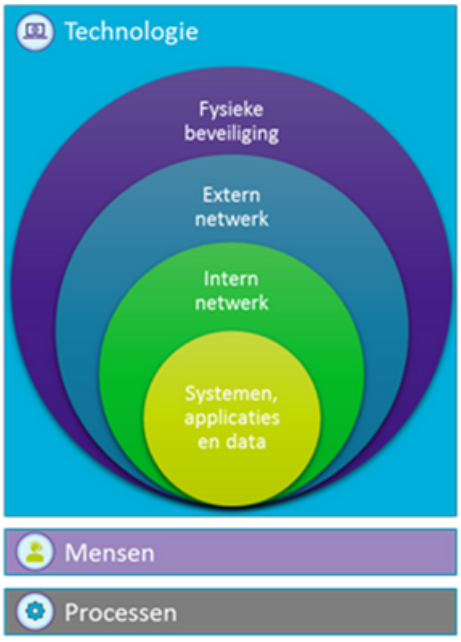
Meer dan 70% van de Nederlandse bedrijven heeft wel eens te maken gehad met cybercriminaliteit. Denk bijvoorbeeld aan phishing e-mails om wachtwoorden of bedrijfsgegevens te verzamelen, of aanvallen met ransomware om alle bedrijfssystemen plat te leggen. In veel gevallen is de schade voor bedrijven enorm. Door langdurig uitval van systemen, lopen de kosten al snel tot in de miljoenen.

De laatste jaren zien we dat het mkb steeds vaker doelwit is van hackers. Bij deze bedrijven is vaak geen overzicht in welke systemen en applicaties bedrijfsgegevens zijn opgeslagen. Ook weten veel ondernemers en IT-afdelingen niet of er voldoende maatregelen zijn genomen om te zorgen dat de gegevens veilig zijn. En is er vaak geen cybersecurity-kennis aanwezig. Hierdoor is het voor hackers heel eenvoudig om in te breken in de systemen.

Wil jij de zekerheid dat hackers bij jouw bedrijf geen ingang vinden? En wil je vertrouwen op een onafhankelijke partij die alle IT-applicaties analyseert? Met de IT security manager van Hoek en Blok.IT speel je op safe. Onze geaccrediteerde register IT-auditors brengen in kaart met welke maatregelen je de beveiliging op orde krijgt én houdt.

Oog voor technologie en mensen

In de basis draait het beveiligen van IT om technologie. Door slimme maatregelen zorg je dat hackers geen toegang krijgen tot systemen en applicaties. Bij Hoek en Blok.IT weten we dat het daar niet stopt. Ook jouw medewerkers en de manier waarop processen zijn ingeregeld, vormen een belangrijk onderdeel van een veilige IT-infrastructuur. Om dit in kaart te brengen, maken we gebruik van een informatiebeveiligingsmodel, gebaseerd op de pijlers technologie, mens en proces.



TECHNOLOGIE

Om jouw techniek goed te beveiligen, werken we van buiten naar binnen. We zorgen voor beveiliging tegen de online buitenwereld, beveiliging van het interne netwerk en het beveiligen van systemen, applicaties en gegevens. Dit doen we door voor alle IT-middelen vast te stellen welke maatregelen nodig zijn om de IT-infrastructuur te beveiligen. Uiteraard richten we de maatregelen vervolgens ook in.

MENSEN

Het klikken op een verkeerde link of het instellen van zeer eenvoudige wachtwoorden: medewerkers zetten vaak onbedoeld de deur wagenwijd open voor hackers. Daarom is het belangrijk dat jouw medewerkers weten welke IT-risico's er zijn en welk gedrag wenselijk is. Onze IT-adviseurs vertellen dit graag en adviseren jouw medewerkers hoe zij invulling geven aan hun IT-beveiligingsverantwoordelijkheid.

PROCESSEN

Om te zorgen dat IT-systemen continu beschikbaar en veilig zijn, heb je goed ingerichte processen nodig. IT-beheer moet bij elk bedrijf een proces zijn, net als bijvoorbeeld HR, inkoop of financiën. Zo krijg je inzicht in je belangrijkste systemen, stel je vast welke maatregelen passen[JP1] bij jouw bedrijf en richt je periodieke controles in.

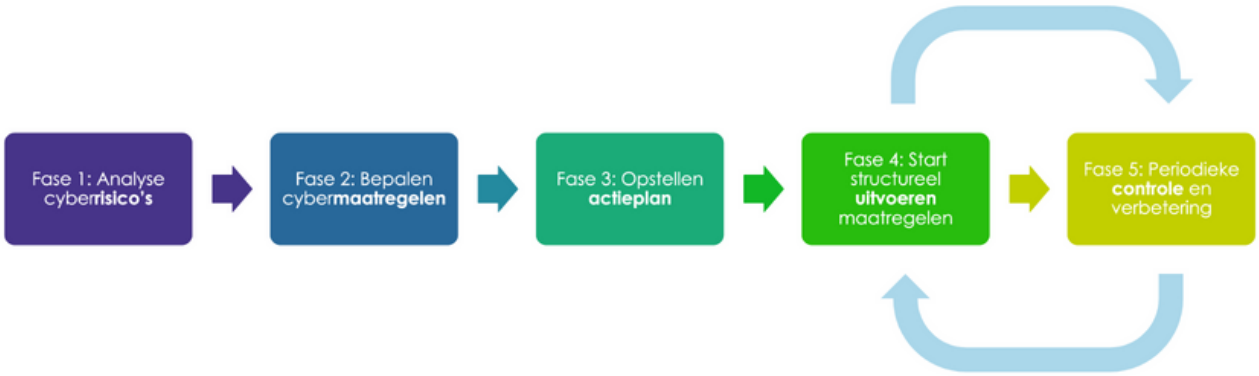
Om inzicht te houden in wie verantwoordelijk is voor welk proces en welke controles maken wij gebruik van toegankelijke tools. Zo houd je weer grip op je bedrijf.

IT security manager: de voordelen op een rijtje

- Goede beveiliging tegen hackers
- Eigen IT-beveiligingsadviseur op afroep
- Snel, schaalbaar en professioneel
- Periodieke controles en bijsturing
- Laag maandtarief

2. In vijf fases naar veilig IT

Wil je de zekerheid dat jouw IT-beveiliging op orde is? Profiteer dan van de voordelen van de IT security manager. Hoek en Blok.IT doorloopt samen met jou en je medewerkers vijf fases om te zorgen dat cybercriminelen geen kans maken om jouw bedrijfsgegevens te stelen.



Fase 1 – Analyse cyberrisico's

In de eerste fase kijken we welke cyberrisico's jouw bedrijf nu loopt. Om dit goed in kaart te brengen, verzamelen we diverse documenten. Denk bijvoorbeeld aan beleidsstukken, procesbeschrijvingen of registratielijsten. Daarnaast stellen we vast welke IT-middelen jouw bedrijf heeft en voeren we technische security testen uit. Zo krijgen we inzicht in de belangrijkste applicaties en weten we hoe jouw IT-infrastructuur en technische beveiliging eruitziet.

Uiteraard hebben we niet alleen oog voor processen en applicaties. Cybersecurity valt of staat met jouw mensen. We willen daarom graag weten welke medewerkers betrokken zijn bij IT, en welke verantwoordelijkheden zij hebben. Ook voeren we een phishing-campagne uit om te beoordelen in hoeverre jouw medewerkers zomaar op een link klikken. Zo hebben we aan het eind van deze fase een goed beeld welke risico's jouw bedrijf op dit moment loopt.

Fase 2 – Bepalen cybermaatregelen

Nu we weten welke risico's jouw bedrijf loopt, is het tijd om vast te stellen welke maatregelen nodig zijn. Hiervoor voeren we een business impact assessment en risicoanalyse uit. Dit doen we om inzicht te krijgen in de kwetsbaarheden van de door jullie gebruikte applicaties en systemen. Vervolgens stellen we vast welk beveiligingsniveau en bijbehorende maatregelen jouw bedrijf nodig heeft om hackers daadwerkelijk buiten de deur te houden.

Fase 3 – Opstellen actieplan
Na het vaststellen van de cybermaatregelen, stellen onze IT-adviseurs een actieplan op met een heldere tijdsplanning, betrokken medewerkers en mogelijke struikelblokken. Het actieplan maakt inzichtelijk welke stappen nodig zijn om te zorgen voor een veilige IT-omgeving. Uiteraard willen wij jouw bedrijf graag helpen met het uitvoeren van de procedures en maatregelen. Hiervoor stellen wij templates en voorbeelden beschikbaar die hun nut in de praktijk hebben bewezen.

Fase 4 – Start structureel uitvoeren maatregelen
Na het doorlopen van de eerste drie fases is het tijd om de nieuwe maatregelen en processen in gebruik te nemen. Om inzicht te krijgen wie welke taken op welk moment moet uitvoeren maken we gebruik van de Procesmanager. Deze tool richten we op maat in voor jouw bedrijf, aangevuld met de proceskennis van onze adviseurs. Zo kun jij erop vertrouwen dat IT-maatregelen tijdig worden uitgevoerd waardoor jouw bedrijf beter in staat is om hackers buiten de deur te houden.

De Procesmanager is overigens ook te gebruiken voor alle andere processen binnen jouw bedrijf. Krijg direct toegang tot de demo-omgeving en ontdek de mogelijkheden.

Fase 5 – Periodieke controle en verbetering
Hackers zitten helaas niet stil. Om te voorkomen dat jouw bedrijf na enkele jaren weer kwetsbaar is, controleren wij periodiek of alle maatregelen en procedures nog op orde zijn. Zo weet jij eerder dan de hacker dat er extra maatregelen nodig zijn.

3. Wat bieden we?

Nieuwsgierig naar de IT security manager en de bijbehorende functionaliteiten en diensten? Neem vrijblijvend contact met ons op.

Het tarief van de IT security manager hangt af van het werkpakket dat hij krijgt. Dit pakket stemmen we samen af op de maatregelen die passend zijn voor jouw bedrijf.

4. Contact

Meer weten?

Neem contact op met onze specialist op dit gebied:

Steven Verkaart RE CISSP CIPP/E
Register IT auditor en IT adviseur
0184 49 68 00
s.verkaart@hoekenblok.IT

Adres

Hoek en Blok Sliedrecht
Stationspark 625
3364 DA Sliedrecht
0184 49 68 00

Hoek en Blok Barendrecht
Tuindersweg 22
2991 LR Barendrecht
0180 64 54 64