E-book

In vijf stappen naar een goede informatiebeveiliging

Heb jij je securitybeleid goed geïmplementeerd?
Toets het met de stappen in dit e-book.

previder

it starts here.

Hoe veilig is jouw IT-omgeving?

Ransomware, hackers, phishing, virussen: er zijn nogal wat gevaren die de veiligheid – en daarmee de integriteit en continuïteit – van jouw IT-omgeving bedreigen. De voorbeelden van organisaties die met dit soort problemen te maken krijgen, liggen voor het oprapen. Met alle gevolgen van dien: van kostbare downtime tot reputatieschade en boetes. Best vreemd dus dat nog steeds zo'n 80% van de organisaties haar informatiebeveiliging niet goed voor elkaar heeft. Hoe zit dat bij jouw bedrijf? Hoe veilig is je IT-omgeving en welke ambities heb je op dat gebied?

Waar moet je starten

Veel bedrijven willen wel werk maken van informatiebeveiliging, maar weten niet waar ze moeten beginnen. Ze missen de focus van bijvoorbeeld een security functionaris, simpelweg omdat ze die geen fulltime functie kunnen bieden. Zodoende is informatiebeveiliging een onderdeel dat veel IT-managers er vaak 'bij' moeten doen.

Uitbesteden dan maar?

Je kunt overwegen om letterlijk alles wat met informatiebeveiliging te maken heeft, uit te besteden. Maar in de praktijk is dat niet werkbaar, want informatiebeveiliging moet één op één aansluiten op jouw bedrijfsprocessen en -beleid. Daar heb je continu input vanuit de organisatie voor nodig. Het volledig overlaten aan een externe partij is dus niet altijd werkbaar, want dat resulteert in een informatiebeveiligingsbeleid dat niet aansluit op jouw organisatie. Hoe dan ook zal je betrokken moeten blijven en misschien wel het meest belangrijke: je organisatie blijft eindverantwoordelijk voor de informatiebeveiliging. Dat kun je niet zomaar verleggen naar een derde partij.

Hoe krijg je als IT-manager je informatiebeveiliging dan wel op orde?

In dit e-book hebben we daarvoor vijf heldere en praktische stappen geformuleerd.

Stap 1

Analyse

Als je op een goede manier aan de slag wilt met IT security, is het essentieel dat je een goed beeld hebt van waar de organisatie nu staat. Is er een visie op het gebied van IT security en informatiebeveiliging, zijn er wettelijke vereisten of standaarden waaraan voldaan moet worden in jouw branche en wat is er beschikbaar op het gebied van budget en middelen? Breng dat soort zaken eens in kaart, zodat je een goed beeld krijgt van de huidige stand van zaken in je organisatie.

- Hoe ziet de huidige IT-omgeving eruit, is hier een helder beeld van?
- Is er een al een beleid of visie op het gebied van IT security of informatiebeveiliging?
- Zijn er compliancyverplichtingen/standaarden waaraan moet worden voldaan en in hoeverre voldoe je daar nu aan?
- Welke (security)maatregelen worden er op dit moment getroffen?
- Is er een analyse gemaakt om te zien wat de impact is op de organisatie wanneer er sprake is van uitval?
- Is er een risicoanalyse gemaakt waaruit blijkt waar de meest zwakke plekken zitten in de organisatie?
- Hoeveel budget en middelen kan en wil jouw organisatie vrijmaken voor informatiebeveiliging?

Om antwoord te krijgen op deze vragen is een Security GAP en een Risico analyse gewenst. Aan de hand van de uitkomst wordt met een security specialist de status besproken.

Stap 2

Vaststellen gewenst beveiligingsniveau

Nu je weet waar je op securitygebied staat, is het tijd om te bepalen waar je naartoe wilt. Hoe groot is het gat tussen wat je nu hebt en wat je graag wilt of juist moet hebben? En wat heb je nodig om je doel te bereiken? Bij het bepalen waar je naartoe wilt, wordt rekening gehouden met het risicoprofiel van de organisatie, het beleid van de organisatie en de gewenste normeringen. Aan de hand van de resultaten uit de Security gap-analyse kunnen vervolgacties gestart worden, die bestaat uit verschillende stappen.

1. Bepaal de securitynorm die je aanhoudt of aan wilt gaan houden

Wanneer je een securitystandaard aanhoudt die geldt voor jouw branche, heb je een soort meetlat waartegen je jouw securitybeleid kunt toetsen. Zo geldt de informatiebeveiligingsnorm NEN 7510 voor de zorgbranche, is er de BIC 3.0 voor woningcorporaties, geldt voor de financiële sector de DORA, houdt de zakelijke markt zich vaak aan de ISO 27001 en zullen veel organisaties te maken krijgen met NIS2.

3. Verzamel relevante data

Hoe effectief is de huidige IT-security en informatiebeveiliging binnen je IT-architectuur? Daarin krijg je inzicht door data te vergaren. Verzamel deze data en pas dataclassificatie toe om een beeld te krijgen van je huidige omgeving.

2. Neem je medewerkers en processen onder de loep

Datalekken en andere securityproblemen zijn vaak het gevolg van menselijk handelen. Denk daarbij aan een medewerker die een link aanklikt in een phishing-email, maar ook aan mensen die uit dienst treden en nog steeds toegang hebben tot het bedrijfsnetwerk. In hoeverre zijn je collega's op de hoogte van de laatste securitybedreigingen en zijn de standaardprocessen ingericht op het voorkomen van datalekken en ongewenste toegang tot bedrijfssystemen? Zijn medewerkers bewust van de risico's? Zo is in NIS2 cyber security awareness en opleiding van de medewerkers een vereiste om compliant te zijn.

4. Analyseren en een plan maken

In dit onderdeel onderwerp je jouw huidige securityprogramma aan een grondige analyse. Wat zijn de sterke punten, waar is verbetering nodig en hoe ga je voldoen aan de securitynorm die je voor ogen hebt? Daarin zijn prioriteiten belangrijk: wat zijn de meest simpele of juist meest kritische punten die direct opgelost kunnen of moeten worden? In het plan wordt rekening gehouden met risico's, mankracht, budget en planning.

Stap 3

Implementeren van benodigde maatregelen

Op basis van het risicoprofiel van de organisatie, het beleid en de gewenste normering, ga je nu de benodigde maatregelen implementeren. Hierbij worden de CIS controls uit het CIS-framework toegepast. De CIS controls zijn een set van ‘best practices’ voor IT-beveiliging, die organisaties helpen hun beveiligingshouding te verbeteren door specifieke maatregelen te implementeren. Deze maatregelen zijn ontworpen om de meest voorkomende en kritische cyberbeveiligingsproblemen aan te pakken.

Begin met het inventariseren van de huidige beveiligingsmaatregelen en identificeer eventuele hiaten. Prioriteer de maatregelen die moeten worden geïmplementeerd en voer zowel technische als organisatorische maatregelen uit. Wanneer deze acties zijn doorgevoerd is hey tijd voor stap 4 waarin je de maatregelen valideert door het uitvoeren van pentesten en vulnerability scans.

Daarnaast is het belangrijk om een Information Security Management Systeem (ISMS) op te zetten of aan te passen. Het implementeren van een managementsysteem kan complex en tijdrovend zijn. Met ons begeleidend implementatietraject krijg je niet alleen advies, maar ook praktische ondersteuning bij elke stap van het proces. Dit traject is ideaal voor organisaties die behoefte hebben aan deskundige begeleiding om de certificering efficiënt en succesvol te behalen.

Stap 4

Pentesten

Nu je een goed beeld hebt van het IT-security beleid en richting binnen jouw organisatie, kun je een heel concrete actie (laten) uitvoeren: een scan van je beveiligingsniveau op dit moment, waarbij de focus ligt op de techniek. Zijn je ramen en deuren gesloten? Zijn er kwetsbaarheden? Zo ja, waar zitten die dan? Om deze vragen te beantwoorden, zijn er verschillende pentestmiddelen in te zetten.

Open Source Intelligence (OSINT pentetration test

Een OSINT pentest helpt bij het identificeren en beperken van informatielekken die kwaadwillenden kunnen misbruiken. Dit type pentest richt zich op het verzamelen en analyseren van publiek beschikbare gegevens over een persoon, bedrijf of organisatie, zonder dat er directe hackingtechnieken worden gebruikt. Het zoekt naar onbewuste blootstelling van gevoelige informatie, zoals gelekte e-mailadressen, wachtwoorden, API-sleutels of documenten die per ongeluk openbaar toegankelijk zijn. Het geeft inzicht in kwetsbaarheden in de digitale voetafdruk en helpt bedrijven om tijdig reputatieschade te beperken.
Tot slot kan een OSINT pentest ook aantonen of een organisatie onbedoeld privacyregels schendt door persoonsgegevens onveilig op internet te laten staan.

Blackbox Pentest

Bij pentesting – voluit: penetration testing – gaan bijvoorbeeld ethische hackers op zoek naar kwetsbaarheden in je IT-omgeving. Als ze iets vinden, proberen ze ook daadwerkelijk binnen te dringen om data te stelen of beschadigen (uiteraard zonder echt schade aan te richten). Een pentest geeft een gedetailleerder beeld dan een vulnerability scan. Het is een uiterst effectief middel om kwetsbaarheden in softwareapplicaties en netwerken op te sporen en te verhelpen.

Stap 4 (vervolg)

Pentesten

Vulnerability scan

Een vulnerability scan is een (meestal geautomatiseerde) check die een globaal beeld geeft van mogelijke zwakke plekken in computers en systemen binnen een bedrijfsnetwerk. Zo'n scan kan eenmalig worden uitgevoerd maar ook volgens een repeterend patroon. Afhankelijk van je IT-omgeving neemt een scan enkele minuten tot enkele uren in beslag. Een vulnerability scan geeft een beeld van kwetsbaarheden maar lost ze niet op. Daar zul jij als IT-manager (of een externe partij die je daarvoor inschakelt) voor moeten zorgen.

M365 Security Scan

De Microsoft 365 Security Scan biedt bedrijven een snelle en geautomatiseerde beveiligingsanalyse van hun Microsoft 365-omgeving. Het identificeert misconfiguraties en beveiligingslekken, vergelijkt instellingen met beveiligingsbaselines, en biedt realtime monitoring en waarschuwingen. De scan genereert gebruiksvriendelijke dashboards en rapportages, ondersteunt compliance en regelgeving, en helpt het risico op datalekken en cyberaanvallen te verkleinen.

Nu alle maatregelen zijn geïmplementeerd en gevalideerd is het van belang dat de security wordt onderhouden zoals in stap 5 wordt beschreven.

Stap 5

Onderhouden

Zodra je volgens de voorgaande stappen je nieuwe informatiebeveiligingsorganisatie hebt opgesteld, ga je op zoek naar een professionele en gespecialiseerde partner voor de implementatie en borging ervan. Kies één partner die je niet alleen adviseert in het maken van de juiste keuzes, maar je ook kan helpen bij het structureel beheren en managen van alles wat met security en risico's te maken heeft. Dit kan bijvoorbeeld ingevuld worden door een CISO-as-a-Service dienst af te nemen. Zo voorkom je dat al je inspanningen beperkt blijven tot een eenmalige exercitie én profiteer je van één aanspreekpunt.

Wat zijn kenmerken van een geschikte IT- en security-partner?

- Gecertificeerde security-experts met up-to-date kennis van zaken;
- Aantoonbare ervaring met het adviseren over en implementeren van een gedegen securitybeleid voor andere (soortgelijke) klanten;
- IT security- en compliancy-oplossingen in huis om er daadwerkelijk voor te zorgen dat jij kunt voldoen aan het beoogde securitybeleid;
- Gecertificeerd volgens de ISO-standaarden;
- Ondersteunend aan informatiebeveiliging NEN-normeringen en BIC-richtlijnen;
- Voorziet in monitoring om continu te blijven toetsen of jouw omgeving veilig is van dreigingen en verstoringen.

Een IT-partner die aan deze voorwaarden voldoet en met wie jij goed kan samenwerken, helpt je bij het realiseren én borgen van een goede informatiebeveiliging voor jouw organisatie. Waarbij jij te allen tijde de regie in handen houdt.

Lig nooit meer wakker van security

(en blijf in control)

Security hoeft niet ingewikkeld en tijdrovend te zijn. Je kunt het ook heel praktisch en doeltreffend aanpakken. Daarbij is het belangrijk dat jij zelf in control blijft. Hierbij is het hebben van een Information Security Management System (ISMS) een belangrijk onderdeel. Een partij met wie jij fijn kunt samenwerken en die het proces pragmatisch benadert, is dan wel zo prettig. Stel kritische vragen en zoek dus een partner uit die bij jou een deskundig en goed gevoel achterlaat. Previder gaat graag eens met je in gesprek om te kijken of er tussen ons een match is.

Certificeringen

Previder is onder andere ISO 27001, 27017, 27018, 14001 en 9001 plus NEN 7510-compliant en BIC 3.0-ondersteunend. Daarmee wordt de beschikbaarheid, integriteit en vertrouwelijkheid van informatie gegarandeerd, met tevens specifieke certificeringen voor de zorg en corporatiemarkt.

Van advies tot implementatie en beheer

Samen met ruim 350 IT-specialisten en vanuit onze eigen datacenters leveren we het gehele IT-fundament voor organisaties. Van digitale werkplekken tot aan het managen van complexe cloudomgevingen. We zijn bovendien strategisch partner en kennisleverancier. We weten de juiste IT-specialist op de juiste plek te zetten en staan 24/7 klaar om jouw organisatie te helpen met IT-vragen.

previder

Meer weten?

Benieuwd wat Previder voor jouw organisatie kan betekenen? We praten er graag eens met je over. Neem contact op voor een vrijblijvende kennismaking.

Previder
088 - 332 3333
info@previder.nl

it starts here.