Informatiebeveiliging Best Practices

Hoe verhoudt uw informatiebeveiliging zich tot industrie best practices?

Hoe effectief is uw Informatie Security Management Systeem (ISMS) in de hedendaagse dynamische omgeving met continue bedreigingen van bijvoorbeeld malware die dagelijks wordt verspreid? De tijd dat u kon vertrouwen op alleen een firewall is helaas voorbij.

De (in)directe kosten van een data-inbreuk kunnen hoog oplopen en grote gevolgen hebben. Verlies of beschadiging van informatie als intellectuele eigendommen, databases, backup-tapes, computer operating systems en data-afhankelijke softwareapplicaties, kunnen een grote impact hebben op de prestaties en reputatie van een bedrijf of organisatie.

Bedrijven zijn tegenwoordig altijd “online” via breedband toegang tot het wereldwijde internet en ook steeds meer afhankelijk van cloud-gebaseerde virtuele omgevingen die beheerd worden door derden. Een ISMS -programma dat voldoet aan industrie best practices maakt uw organisatie minder kwetsbaar voor aanvallen en significante (financiële) schade.

Best practices

Effectieve informatiebeveiliging beschermt uw intellectuele eigendommen en data tegen bedreigingen, waarborgt de continuïteit van uw bedrijf, beperkt bedrijfsschade en verhoogt het rendement op investeringen. Er zijn vele best practices die aan de kwaliteit van uw ISMS programma kunnen bijdragen. Het voornaamste is echter dat risicobeheersingsmaatregelen relevant zijn voor, en goed aansluiten op, uw specifieke bedrijfsrisico’s. Hieronder brengen wij een aantal (essentiële) aspecten onder de aandacht.

Betrokkenheid management

- Introduceer een cultuur van informatiebeveiliging en handhaaf deze in de gehele organisatie, zowel binnen het management als bij de medewerkers.
- Maak iedereen verantwoordelijk voor zijn eigen handelingen met betrekking tot informatiebeveiliging.
- Stel één aanspreekpunt aan voor alle informatiebeveiligingsthema’s.
- Beheer informatiebeveiligingsrisico’s voor

zowel interne als externe bedreigingen.
- Blijf bestaande bedreigingen herbeoordelen en monitor en beoordeel ook doorlopend nieuwe bedreigingen. Let vooral ook op de toenemende web-based bedreigingen.
- Dwing mensen om zich aan beleidsmaatregelen en procedures te houden.

Risicobeoordeling

- Zorg dat u een compleet beeld heeft van alle interne en externe informatiebeveiligingsrisico´s en de continu veranderende aanvallen op uw organisatie. Het is van essentieel belang precies te weten waar informatie zich bevindt en hoe deze bedreigd kan worden.
- Analyseer welke impact deze informatiebeveiligingsrisico's kunnen hebben op uw netwerk, processen, bedrijfsmissie en reputatie.
- Identificeer uw bedrijfs(data)bezittingen en leg, met behulp van de pijlers beschikbaarheid, integriteit en vertrouwelijkheid (BIV), vast hoe kritisch deze data is.
- Zorg dat u te allen tijde weet waar deze data zich bevindt, zowel binnen als buiten (cloud) de organisatie.
- Bescherm kritische data met behulp van versleuteling of andere hiervoor geschikte middelen, zowel binnen als buiten(cloud) de organisatie.
- Beoordeel per proces de risico´s en ken hier een waarde aan toe. Houd hierbij rekening met eventuele onderlinge en overkoepelende samenhang. Bij het beoordelen van de risico´s dient tevens rekening te worden gehouden met eventuele beveiligingsproblemen en de impact die deze kunnen hebben op de bedrijfsvoering.
- Ga bij het beoordelen van de risico´s uit van de drie eerder genoemde pijlers (BIV). Kwetsbaarheden hangen mede af van:
  - Managementbeleid
  - Fysieke omgeving
  - Scheiding van verantwoordelijkheden en beslissingsbevoegdheden
  - Opleiding en screening van personeel
  - Administratieve procedures, penetratietesten, audits etc.
  - Hardware, software en communicatieapparatuur
  - Thuiswerkers, draadloze verbindingen en zgn. "endpoint" beveiliging.

  Voer regelmatig kritische herbeoordelingen van uw data uit.

Vertrouwelijkheid en privacy

- Categoriseer data in risicoklasses. Ga hierbij uit van het eerder aangegeven BIV-model en houd hierbij rekening met zowel interne als externe (cloud) data. Stel per risicoklasse beveiligingsmaatregelen vast.
- Stel beleidsmaatregelen op voor toegang tot "persoonlijke" data. Voorbeelden hiervan zijn toegangsrechten, authenticatie controlemaatregelen, data backup, redundante opslag en versleuteling van data.
- Zorg ervoor dat "gevoelige" data altijd adequaat wordt beveiligd. Houd extra toezicht op data opgeslagen bij derden (in de Cloud, bij zakenpartners etc.).
- Zorg dat databestanden bijgewerkt zijn en regelmatig opgeschoond worden.
- Ga regelmatig na of u nog voldoet aan alle wettelijke en contractuele vereisten met betrekking tot uw activiteiten.
- Voer allesomvattende authenticatie- en autorisatiebeveiligingsmaatregelen in die de toegang tot gevoelige informatie beperken.
- Zorg dat u voldoet aan van toepassing zijnde wettelijke en regulatory eisen zoals de Payment Card Industry (PCI) standard en eventuele eisen van buitenlandse organisaties. Huur eventueel een gekwalificeerd persoon in die u hierbij kan helpen.
- Zorg dat u beschikt over een data incident respons plan. In een dergelijk plan dienen afspraken te worden vastgelegd over te volgen procedures in geval van verlies of diefstal van data. Bijvoorbeeld informatie met betrekking tot melding van een inbreuk aan de Autoriteit Persoonsgevevens.

Documentatie en implementatie van beleidsmaatregelen en procedures

- Creëer en onderhoud dynamische security beleidsmaatregelen waarin alle interne en externe virtuele en niet virtuele omgevingen zijn opgenomen.
- Houd een lijst bij van alle potentiële en gewezen incidenten en alle (on)opzettelijke dreigingen.
- Zorg voor een "acceptable use policy" (gebruiksregels) voor medewerkers.
- Implementeer een patch management programma en zie toe op de naleving.
- Zorg voor systemen die automatisch toegang tot sites monitoren en eventueel toegang tot ongewenste sites blokkeren.
- Zorg voor een robuust continuïteits- en disaster recovery plan en test dit regelmatig.
- Beveilig of blokkeer instant messaging (IM).
- Voer vooraf en direct na overnames en fusies een network security analyse uit.
- Ontwikkel een business continuïteitsplan (BCP). In een dergelijk plan worden procedures vastgelegd die kunnen worden uitgevoerd in geval van een onderbreking van uw activiteiten

door bijvoorbeeld het niet beschikbaar zijn van systemen.

Personeels –en gebouwbeveiliging

- Voer een gedegen screening uit voor nieuw personeel en wees extra zorgvuldig bij kritische functies zoals netwerk administrators en personeel dat toegang heeft tot gevoelige data.
- Definieer en documenteer individuele rollen en verantwoordelijkheden voor informatiebeveiliging in de organisatie.
- Bied continu trainingen aan over informatiebeveiliging om de bewustwording te verbeteren en te voorkomen dat niet voldaan wordt aan ingevoerde procedures. Trainingsonderwerpen kunnen onder andere zijn:
  - Actuele bedreigingen
  - Social engineering
  - Phishing
  - Posting blogs
  - Goede paswoorden
  - Clear screen en desk policy
  - P2P (Peer-to-Peer) and social media risico´s
  - Externe opslagmedia (USB etc.)
  - Rapporteren van inbreuken en fouten
  - Bring Your Own Device (BYOD)
- Maak voor veilige wachtwoorden gebruik van minimaal 8 alfanumerieke tekens bestaande uit een mix van tekens, cijfers en hoofdletters. Wijzig wachtwoorden elke 60 dagen en sta hergebruik van paswoorden binnen 24 cyclussen niet toe.
- Zorg voor een goede beveiliging van uw gebouwen en (computer)ruimtes door het treffen van organisatorische, bouwkundige en elektronische maatregelen. Een goede afstemming tussen fysieke en logische beveiliging is noodzakelijk.
- Voor kritische IT-infrastructuur dient overwogen te worden om een UPS (Uninterruptable Power Supply) of noodstroomaggregaat aan te schaffen.

Beheer van netwerk en systemen door toepassing van technologie

- Creëer meerdere beveiligingslagen, met up-to-date, goed geconfigureerde firewalls.
- Zorg voor up-to-date, geautomatiseerde malwaredetectie-en preventiesystemen, gebaseerd op signatuur en gedrag.
- Versleutel databases, laptops en data die over het internet gaan.
- Maak gebruik van anti-spyware om malware op uw systemen te voorkomen.
- Als u spyware op uw computer aantreft, zorg er dan voor dat deze niet kan communiceren buiten uw eigen netwerk zodat het geen verdere instructie kan ontvangen of uitzenden.
- Zorg dat uw website veilig door uw gebruikers gebruikt kan worden, maar sluit uw netwerk af voor onbevoegde derden. Gebruik perimeter beveiligingssoftware, software om het gedrag van gebruikers te monitoren en software om datalekken te voorkomen.
- Beveilig “endpoints” binnen en buiten de organisatie en let hierbij specifiek op Wifi.
- Voorkom aanvallen op VoIP (Voice over Internet Protocol) door gebruik te maken van een veilig PBX (Private Branch Exchange).
- Zet specifieke tools in en maak gebruik van redundante internet service providers om Ddos (Distributed Denial of Service)- aanvallen te bemoeilijken.
- Maak regelmatig een back-up van data (en software). Zorg ervoor dat dit in de hele organisatie gebeurt en test de back-up regelmatig. Bij voorkeur dienen procedures vastgelegd te worden in een Disaster Recovery Plan (DRP).
- Gebruik technologie en procedures om het (on)opzettelijk verwijderen, veranderen of toevoegen van kritische databestanden te voorkomen.
- Voer een formele patching procedure in.
- Werk regelmatig VPN firewalls en anti-virus detectie bij op alle mobiele toestellen.
- Aanvullende beveiligings-maatregelen kunnen bestaan uit een Intrusion Detection Systeem (IDS), Intrusion Prevention Systeem (IPS) of Security Information and Event Management systemen (SIEM).

Monitor en audit

- Voer een zogenaamde nulmeting van uw netwerk uit om vast te stellen wat de normale basisactiviteiten zijn.
- Monitor alle activiteiten op het web en blokkeer toegang tot ongepaste websites en websites met een hoog risicoprofiel.
- Voer regelmatig penetra-tietesten uit in overeen-stemming met het risico.
- Monitor regelmatig of nieuwe software wordt geüpload en check deze op zwakheden.

Afwegingen m.b.t. outsourcing en cloud

- Beoordeel welk werk wordt uitbesteed aan derden en stel degelijke Service Level Agreemeents (SLA) op met daarin vastgelegd wie toegang mag hebben tot welke informatie. Leg dit ook vast in een eventuele bewerkers-overeenkomst.
- Beoordeel en documenteer het risico van misbruik of verandering

van data en het niet beschikbaar zijn van IT-systemen, die al uitbesteed zijn aan derden voordat de activiteiten daadwerkelijk starten.

- Verlang van derden dat zij dezelfde procedures handhaven als de interne organisatie en controleer dit regelmatig via audits.
- In (bewerkers)overeenkomsten dienen minimaal de volgende zaken vastgelegd te worden: verantwoordelijkheden, verwachtingen en meldings – en escalatieprocedures met betrekking tot data. Houd hierbij rekening met de vereisten uit de Wet bescherming persoonsgegevens en de Meldplicht datalekken.
- In aanvulling op bewerkersovereenkomsten dient er regelmatig een formele evaluatie plaats te vinden van de veiligheidsprocedures bij de dienstverlener met bijzondere aandacht voor de vereisten vanuit de privacywetgeving.
- Leg contractueel procedures vast (eventueel in de bewerkers-overeenkomst) over hoe apparatuur, software en data, na de looptijd van het contract, geretourneerd dient te worden.
- Zorg dat u op de hoogte bent van uw opties met betrekking tot outsourcing. Welke alternatieve leveranciers zijn er? Is er een exit-strategie vastgelegd? Wie is eigenaar van de data?

Samenvatting

Voor een succesvol ISMS (Information Security Management Systeem) is een dynamisch en veelzijdig risicomanage-mentbeleid noodzakelijk. Industrie Best Pratices bieden goede houvast bij het ontwikkelen van een succesvol systeem, dat tevens goed dient aan te sluiten op uw specifieke beveiligingsrisico's. Ook na implementatie dienen risico's continu gemonitord en herbeoordeeld te worden om aanvallen te voorkomen en/of het risico hierop te beperken.

Voor vragen en/of aanvullende informatie, neem contact met ons op

Chubb
Siriusdreef 2
2132 WT Hoofddorp
Nederland
T 0235661800
F 0235651371
www.chubb.com

Wouter Wissink
Property & Casualty Risk Engineer & INT Specialist, Risk Engineering Services
T +31 (0)23 5661 832
E wwissink@chubb.com

Chubb. Insured.℠