Den Ouden Informatiebeveiliging
Van Foreestallee 53
7773 DC Hardenberg
info@denoudeninformatiebeveiliging.nl
06-34822893

KvK-nr.: 63279622
Btw-nr.: 855167051b01

IBAN: NL24RABO0303494387

Menukaart

Hieronder vind je een overzicht van de producten die Den Ouden Informatiebeveiliging kan aanbieden. We hebben ons aanbod hieronder uiteengezet in de vorm van een “menukaart”. Je kunt dus zelf mixen-en-matchen. Neem gerust contact met ons op voor het maken van een passende offerte.

Basis security-check in een dag
Gedurende een dag inventariseren we de stand van zaken op het gebied van security aan de hand van een checklist. Aan het einde van de dag zullen we een presentatie houden over de uitkomst van het onderzoek. Dit onderzoek geeft ook een goede basis voor andere testen die uitgevoerd kunnen worden zoals een pentest, awareness sessie of het maken van beleid. Waar staat je organisatie op het gebied van security en privacy, en waar kan er nog een verbetering plaatsvinden?

Onderwerpen die aan bod komen zijn:

- Organisatie & Governance
- Gedrag & Cultuur
- Waardeketen versus Risico’s
- Verantwoordelijkheden
- Wet- en Regelgeving
- Beleid
- Detectie van een incident
- Reactie op een incident

Incident Handling & Response

Een kwetsbaarheid zit in een klein hoekje en het kan natuurlijk altijd voorkomen dat het toch misgaat. Wat doe je dan? In zeven stappen kun je van incident naar recovery en uiteindelijk response gaan. Hiervoor maken we de documentatie, stellen de plannen en procedures op en zorgen dat er getraind wordt zodat alle betrokkenen begrijpen wat er gedaan moet worden als er een incident plaatsvindt. Afhankelijk van het soort bedrijf, de grootte van de organisatie, de wens en wat al aanwezig is wordt bepaald wat de doorlooptijd is.
Een IHR traject bevat in ieder geval de volgende onderdelen:

- Voorbereiding: scope bepalen, inventarisatie van documenten en beleid
- Incidentregistratie: hoe wordt dit gedaan? Een prioriteit geven aan het incident.

- Notificatie: welke partijen moeten worden geïnformeerd?
- Incidenten insluiten
- Bewijsmaterialen verzamelen, analyse
- Incidenten wissen/uitroeien
- Herstel (recovery)
- Post incident acties

Pentesten en security scans

Den Ouden Informatiebeveiliging kan verschillende testen aanbieden om computersystemen, netwerken, software (zelfbouw en ingekocht), web en app te testen op kwetsbaarheden. We doen dit in de volgende vormen:

- **Basis security scan**
    - Snelle scan die inzicht geef in meest voorkomende kwetsbaarheden
    - Voor (maatwerk) software: veel gebruikt tijdens het testen in startfase van ontwikkeling of tijdens een SCRUM traject.
    - Netwerken: geeft een overzicht van het netwerk, gebruikte systemen, protocollen, gebruikte services, etc.
    - Geeft direct overzicht in de huidige stand van zaken m.b.t. security
    - Rapportage in de vorm van een beknopt overzicht van kwetsbaarheden.

- **Pentest**
    - Pentest waarbij Den Ouden Informatiebeveiliging toegang krijgt tot een (afgeschermd) deel van de applicatie (web, app, systeem, netwerk, ip-adres etc) en duidelijk wordt afgesproken (in contract) wat wel en niet getest moet worden en wat binnen de scope valt van deze test.
    - Buiten de scope vallen in ieder geval: DoS aanval op productieomgevingen
    - White-Box variant: Er worden (minimaal) twee accounts beschikbaar gesteld door de organisatie waarmee getest mag worden. Verder is alle documentatie beschikbaar zoals werktekeningen, broncode, etc. Er kan tijdens de test contact gezocht worden met de organisatie om vragen te stellen over de werking van de omgeving die getest wordt.
    - Grey-Box variant: deze test geeft een gebied aan waar getest mag worden en een account waar getest mee mag worden. Het simuleert een aanval waar de kwaadwillende hacker toegang heeft gekregen tot een systeem en zichzelf verder toegang probeert te verschaffen.
    - Black-Box variant: er worden geen accounts verstrekt en Den Ouden Informatiebeveiliging gaat aan het werk zoals een kwaadwillende hacker ook zou doen.

Deliverables:

- Rapportage in de vorm van een uitgebreid rapport waarin alle technische details besproken worden, advies wordt gegeven en alle ruwe data ter beschikking wordt gesteld. Aangevuld met een managementsamenvatting en risicoanalyse.
- Deze test kan worden aangevuld met:
  - Een audit rapport t.b.v. ISO 27001, NEN 7510
  - Third Party Mededeling t.b.v. AVG en/of DPIA

Alle hierboven genoemde testen worden uitgevoerd conform OWASP Top 10 en volgens de richtlijnen van NCSC.

Uiteraard wordt er gewerkt met een Non-Disclosure Agreement (NDA, waiver) en waar nodig een Letter of Authority. Hierin staat wat de Den Ouden Informatiebeveiliging test, wie de belanghebbenden zijn, en de algemene geheimhouding die Den Ouden Informatiebeveiliging heeft ten aanzien van andere partijen. De resultaten worden enkel gedeeld met de organisatie. De opdracht gevende partij blijft in control en kan de testen altijd stoppen.

Applicatie Privacy Check

Maakt je organisatie software? Of koop je maatwerk software in? Dan is de kans groot dat deze software persoonsgegevens verwerkt. Het is dan goed om te weten waar risico's kunnen liggen wanneer dit niet veilig of foutief gedaan wordt.

Aan de hand van een checklist gaan we langs de verschillende mogelijkheden die de software biedt: waar sla je bijvoorbeeld gegevens op en wat mag wel wat mag niet? De checklist kan gebruikt worden als input voor een DPIA en geeft direct inzicht in de verwerking van de applicatie. Ook weer handig als basis voor bijvoorbeeld een verwerkingsregister.

Er wordt gekeken naar:

- Dataclassificatie
- Privacy by design en privacy by default
- Mate van security (security by design)
- Wijze van opslag
- Transport van data
- Locaties
- Encryptie
- Gebruikte tooling

Mysterybezoek (Social Engineering)

Uit onderzoek blijkt dat veel security incidenten binnen de organisatie niet digitaal zijn. Vaak is het onwetendheid of onbewust gedrag van de medewerker zelf die zorgt voor een security incident.

Kwaadwillende hackers maken daar graag gebruik van en leiden medewerkers om de tuin om hun slag te kunnen slaan. Dit wordt Social Engineering genoemd

We kunnen afspreken welke van de onderstaande mysterybezoeken we gaan uitvoeren.
De mogelijkheden:

- USB drop: er wordt een USB-stick afgeleverd bij de receptie. Deze USB-stick geeft een signaal door aan den Ouden Informatiebeveiliging wanneer deze in een computer gestoken is. De juiste reactie van de receptiemedewerker zou zijn om de USB-stick niet te gebruiken.
- Vishing – voice phishing: we gaan bellen met de service desk om te kijken of we een wachtwoord kunnen achterhalen of wijzigen. Ook zouden we met een andere afdeling kunnen bellen om te bekijken welke bedrijfsinformatie we kunnen achterhalen.
- Mystery-bezoek: tijdens dit bezoek proberen we om het pand ongeautoriseerd binnen te lopen. Tijdens het bezoek proberen we diverse dingen:
    - Bijvoorbeeld een Wifi-Pineapple te plaatsen op een plaats zouden mensen hierop inloggen en we informatie kunnen onderscheppen.
    - Prints meenemen van een printer.
    - Een netwerkscanner plaatsen die het netwerk scant en informatie doorsluist naar een externe computer.
- Geprepareerde USB-stick inpluggen in bedrijfsapparatuur waarbij wachtwoorden te achterhalen zijn.
- Briefpapier proberen mee te nemen, hiermee zou een kwaadwillende een brief kunnen sturen naar een klant waarbij hij probeert om geld te ontvangen.

Uiteraard wordt er gewerkt met een Non-Disclosure Agreement (NDA). Hierin staat wat Den Ouden Informatiebeveiliging test, wie de belanghebbenden zijn, en de algemene geheimhouding die Den Ouden Informatiebeveiliging heeft ten aanzien van andere partijen. De resultaten worden enkel gedeeld met de organisatie. De opdrachtgevende partij blijft in control en kan de testen altijd stoppen.

Phishing mail
Er kan een phishing mailcampagne voor alle medewerkers van de organisatie worden opgezet. De mail wordt opgesteld aan de hand van de volgende criteria:

- Template (look & feel) is gelijk aan die van een legitieme mail zoals de medewerker gewend is. Dit kan vanuit de organisatie zijn of vanaf een leverancier of klant.
- De e-mail houdt bij door wie en wanneer de phishing mail is geopend. Er kan daarnaast bekeken worden welke gegevens zijn afgestaan. Dit is een stap extra waarbij de mail wordt voorzien van bijvoorbeeld een portaal waar de medewerker op kan inloggen.
- Resultaten kunnen real-time worden bekeken. Er kan dus bekeken worden wat er met de mail gedaan wordt (wordt deze bijvoorbeeld doorgestuurd, geopend, weggegooid, welke data wordt er verstuurd, etc.).

- Er kan toegang gegeven worden aan je organisatie om mee te kijken op het dashboard zodat resultaten al direct zichtbaar zijn.
- Rapportage wordt hierna opgemaakt.

Goed om te weten: Den Ouden Informatiebeveiliging kiest ervoor om uit ethisch oogpunt wachtwoorden niet in te zien, op te slaan of op welke manier dan ook te verwerken die door de medewerkers zouden kunnen worden verstrekt tijdens de phishing mailcampagne.

Uiteraard wordt er gewerkt met een Non-Disclosure Agreement (NDA). Hierin staat wat de Den Ouden Informatiebeveiliging test, wie de belanghebbenden zijn, en de algemene geheimhouding die Den Ouden Informatiebeveiliging heeft ten aanzien van andere partijen. De resultaten worden enkel gedeeld met de organisatie. De opdracht gevende partij blijft in control en kan de testen altijd stoppen.

Trainingen

Den Ouden Informatiebeveiliging biedt verschillende trainingen op het gebied van security en privacy aan. Hieronder een beknopt overzicht:

Jochen is officieel Certified EC-Council Instructor. Daarom mag hij de volgende trainingen geven:

- EC-Council Certified Ethical Hacker (CEH). In vijf dagen leer je de ins en outs van het (ethisch) hacken. Je krijgt inzicht in de tools die de hacker gebruikt en als je het examen doet mag je jezelf CEH noemen. Meer info: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
- EC-Council Certified Incident Handler. Waar liggen je grootste dreigingen en wat moet je doen na een incident of aanval? In deze training leer je hoe je moet handelen voor, tijdens en na een databreach. Binnen drie dagen wordt je klaargestoomd voor het officiële examen.Meer info: https://www.eccouncil.org/programs/ec-council-certified-incident-handler-ecih/
- Onze eigen training Hacker:404 (1 dag): Krijg de mindset (en vaardigheden) van een hacker in slechts één dag. Dat is wat Hacker:404 doet. Er komen verschillende onderwerpen aan bod die worden toegelicht aan de hand van tekst, beeld en film. Daarnaast worden de aanwezigen uitgedaagd om na te denken over en te discussiëren over verschillende onderwerpen. Waar zijn ze het mee eens? En welke niet?
    - De training richt zich vervolgens op verschillende tools die door hackers worden gebruikt. We starten met een aantal demo's, waarna de cursisten zelf aan de slag gaan in verschillende (kwetsbare) omgevingen. Zo leren ze werken en denken als een hacker. Je gaat dus echt hacken.
    - Hacker: 404 is een training voor kleine groepen die 1 dag duurt en maximaal 10 personen per training kunnen deelnemen.
- Training AVG/GDPR: meer weten over privacy en de wet AVG (GDPR)? Dan is deze training echt iets voor je organisatie. Deze training is niet saai en wollig maar juist to-the-point met

veel voorbeelden en praktijkvoorbeelden. Dit zorgt voor een fijne training waarbij je meer resultaat boekt en die direct toepasbaar is. Deze training werd inmiddels verzorgt voor meer dan 100 klanten.

Presentaties, lezingen en awareness sessies

Datalekken. Cybercrime. Hackers. Zo maar wat termen die dagelijks in het nieuws voorbijkomen. Hoe zit het nu eigenlijk? Wat is een hacker? Waarom is het publiek interessant voor een hacker? In een interactieve talk ga met het publiek door het landschap van cybersecurity en privacy. Ik laat zien wat mijn werk als IT Security Specialist inhoudt. In een aantal demo's laat ik zien hoe een hacker te werk gaat, welke informatie het publiek deelt (ter plekke) en geef ik handvatten zodat het publiek direct aan de slag kan met hun eigen cyberveiligheid.

Wat anderen zeiden over een lezing:

Onlangs heeft Jochen tijdens onze Xiphos klantendag én personeelsbijeenkomst een interessante presentatie gegeven over IT-Security. Jochen wist alle aanwezigen tot het einde aan toe te boeien. Iedereen werd toch wel even wakker geschud door zijn verhaal. Hij heeft ontzettend veel kennis van IT-Security en passie voor zijn vak. Dit maakt dat hij vol enthousiasme zijn verhaal kan vertellen. Niet alleen een duidelijk verhaal, maar ook praktijkvoorbeelden. Hij vertelt dit op een prettige manier, waardoor het voor iedereen (IT'er of niet) goed te volgen is. Jochen is daarnaast iemand met wie je goed kunt schakelen. Onze samenwerking was erg prettig. Voor herhaling vatbaar. Cynthia Bruinsma, Xiphos B.V.

Jochen tijdens het Techniek&Innovatie evenement Innofuture een Tech-Talk over Hacken verzorgd. Opeen deskundige, enthousiaste en interactieve manier nam hijbezoekers mee in de wereld van Hacken. Van jong tot oud hingen aan zijn lippen! Linda Meijer-Alberts, Stichting Innofuture

Tijdens onze 2-jaarlijkse veiligheidsdag BRANDstof tot nadenken heeft Jochen tijdens de 4e editie een 1 uur durende lezing gegeven over zijn vakgebied: ethisch hacken en veilige ICT. Bevlogen, enthousiast en zijn zeer ruime ervaring spatten ervan af. Erg interessant en onze gasten waren dan ook zeer tevreden. Als u een spreker zoekt die u de ogen kan openen omtrent hacken, dan moet u Jochen zeker eens aanhoren. - Marnix Arentsen, Signs & Safety

Consultancy

Den Ouden Informatiebeveiliging biedt advies aan in de vorm consultancy. Tijdens een consult wordt gekeken naar specifieke vragen die je als organisatie hebt. Onderwerpen kunnen zijn:
- Huidig en nieuw beveiligings- en privacybeleid (AVG/GDPR)
- Advies over IAM
- Rapportages (scans, bevindingen, etc.)
- Gedrag van werknemers in termen van ondersteuning voor privacy en veiligheid en voldoen aan het beleid op dit gebied.
- Prioriteiten stellen met betrekking tot zowel beveiliging als privacy.

- Uitrollen van nieuw beleid.
- Het draagvlak voor informatiebeveiliging creëren bij je medewerkers.
- Securityvraagstukken; waar moet je op letten? Welk product past het beste binnen je organisatie, etc.
- Hoe om te gaan met bijvoorbeeld “Privacy by Design”, “Privacy by Default” en “Security by Design”
- Vragen m.b.t. AVG en ook bijvoorbeeld Baseline Informatiebeveiliging Overheid (BIO)