LAWRENCE
DATA PROTECTION · AI · TECH

HUNT & HACKETT

Is jouw incident response proces klaar voor het huidige EU-meldlandschap?

EEN ZELFEVALUATIE IN 6 STAPPEN

Stap 1 → Gebeurtenis: wat is er waargenomen?
Kan jouw securityteam in de eerste uren een betrouwbaar eerste beeld opleveren?

- ☐ Wij kunnen snel vaststellen welke systemen zijn geraakt en in welke volgorde
- ☐ Onze logging en telemetrie zijn toereikend om een eerste aanvalstijdlijn te reconstrueren
- ☐ Wij weten welke systemen buiten onze monitoringscope vallen
- ☐ Wij kunnen het type incident in een vroeg stadium onderscheiden — ransomware, datadiefstal, BEC, espionage — omdat de respons per type verschilt
- ☐ Wij documenteren vanaf het eerste moment wat is vastgesteld, wat aannemelijk is en wat nog open staat
- ☐ Wij kunnen binnen 24 uur vaststellen welke interne en externe stakeholders betrokken moeten worden bij de besluitvorming

Stap 2 → Mogelijke regimes: welke wetgeving komt in beeld?
Voert jouw legal- of complianceteam een regime-scan uit voordat een meldbeslissing wordt genomen?

- ☐ Wij weten onder welke EU-regimes onze organisatie valt: AVG, NIS2, DORA, CRA en/of AI Act
- ☐ Wij voeren bij ieder incident een korte horizon-scan uit op drie assen: data, dienstverlening en technologie
- ☐ Wij weten welke toezichthouder bij welk regime hoort
- ☐ Wij begrijpen dat één incident meerdere juridische identiteiten kan hebben en handelen daar ook naar
- ☐ Wij hebben in kaart gebracht welke systemen, bedrijfsprocessen en datacategorieën onder welk regime vallen

Stap 3 → Forensische feiten: wat is er daadwerkelijk gebeurd?
Levert jouw forensisch onderzoek een feitenbeeld op dat juridisch interpreteerbaar is?

- ☐ Wij hebben directe toegang tot forensische expertise op het moment dat een incident zich voordoet
- ☐ Wij kunnen tijdens een lopend incident onderzoeksprioriteiten bepalen zonder de continuïteit van containment en herstel uit het oog te verliezen.
- ☐ Wij kunnen een initiële root cause analyse uitvoeren terwijl containment nog loopt
- ☐ Wij stellen per bevinding expliciet vast wat zeker is, wat aannemelijk is en wat nog open staat
- ☐ Wij kunnen reconstrueren wanneer initiële toegang plaatsvond, los van het moment van detectie

Stap 4 → Juridische kwalificatie: welke meldplichten worden getriggerd?
Kan jouw legal-team op basis van het forensisch feitenbeeld een verdedigbare juridische kwalificatie maken?

- ☐ Onze legal- en forensische teams hanteren een gemeenschappelijke incidenttaal
- ☐ Wij werken met evidence-based voorlopige kwalificaties en wachten niet op volledige zekerheid
- ☐ Wij begrijpen het verschil tussen de meldtermijnen per regime en weten wanneer die beginnen te lopen
- ☐ Juridische triggers worden vertaald naar concrete forensische onderzoeksvragen en andersom
- ☐ Wij hebben gedefinieerde besluitvormingsmomenten voor de eerste 4, 24 en 72 uur

Stap 5 → Melding(en): aan de juiste autoriteit, in de juiste vorm, binnen de juiste termijn
Is jouw meldproces ingericht op meerdere parallelle meldsporen?

- ☐ Wij hebben vooraf vastgesteld wie bevoegd is om meldingsbesluiten te nemen
- ☐ Wij weten hoe wij een vroege waarschuwing, een incidentmelding en een eindverslag van elkaar onderscheiden
- ☐ Wij kunnen een technisch onderbouwde melding doen terwijl het forensisch onderzoek nog loopt
- ☐ Wij hebben escalatielijnen gedefinieerd die forensische én juridische expertise vanaf het eerste uur activeren
- ☐ Wij hebben eerder geoefend met het opstellen van een melding onder tijdsdruk
- ☐ Wij bewaken actief de cadans van vervolgmeldingen en tussentijdse verslagen

Stap 6 → Bewijsdossier: kan de besluitvorming achteraf worden gereconstrueerd?
Bouw jij tijdens het incident al het dossier op waarmee je achteraf verantwoording kunt afleggen?

- ☐ Wij bouwen tijdens een incident actief een bewijsdossier op, niet achteraf
- ☐ Ons dossier bevat per besluitvormingsmoment een expliciete kennisstatus: wat wisten wij toen, wat niet, en waarom
- ☐ Wij kunnen verantwoorden waarom een melding wel of niet is gedaan op een bepaald moment
- ☐ Forensische bevindingen en juridische kwalificaties worden in hetzelfde dossier bijgehouden
- ☐ Toezichtsrapportage en juridische review worden behandeld als doorlopend spoor, niet als afsluiting van het incident

Wat zegt de uitkomst?
De checklist is geen eindoordeel. Hij laat zien waar het incident response proces stevig staat en waar het onder tijdsdruk waarschijnlijk onder druk komt te staan.

Ontbreken vinkjes vooral in stap 1, 3 of 6?
De technische basis verdient aandacht. Denk aan logging, retentie, forensische capaciteit en de kwaliteit van het eerste feitenbeeld. Dat zijn de bouwstenen die bepalen hoe verdedigbaar jouw positie is op het moment dat een toezichthouder vragen stelt.

Ontbreken vinkjes vooral in stap 2, 4 of 5?
De juridische kalibratie verdient aandacht. Denk aan regime-mapping, melddrempels en de vraag of de escalatielijnen snel genoeg de juiste expertise activeren.

Ontbreken vinkjes verspreid over meerdere stappen?
Dan loopt techniek en juridisch niet in de pas — en dat is precies de situatie waarin organisaties onder druk uit de pas raken.

Wil je weten of jouw beeld klopt? Hunt & Hackett en Lawrence Advocaten denken graag met je mee.

LAWRENCE
DATA PROTECTION · AI · TECH

Lawrence is een vooruitstrevend advocatenkantoor gespecialiseerd in Data (Protection), AI & Tech. Wij geloven dat juridische expertise niet stilstaat, maar meebeweegt met de wereld van morgen. Daarom combineren wij diepgaande kennis met creativiteit en technologie om cliënten te helpen kansen te benutten én risico's te beheersen.

🔗 www.lawrence-advocaten.nl
www.linkedin.com/company/lawrence-advocaten/
+31 6 2079 1755

HUNT & HACKETT

Hunt & Hackett is een cybersecuritybedrijf dat Europese bedrijven beschermt tegen digitale dreigingen en spionage. Wij opereren als managed detection & response (MDR) en incident response partner, met specialisten die dagelijks aan de frontlinie van cyberconflicten staan om organisaties te helpen bij het voorkomen van, herkennen van én reageren op cyberaanvallen.

🔗 www.huntandhackett.com
www.linkedin.com/company/huntandhackett
+31 70 222 0000