

CYBERSECURITY CHECKLIST

Het meest onderschatte probleem in cybersecurity-landschap

Als jij dit hebt aangevraagd, ben je waarschijnlijk een security-verantwoordelijke. Je bent lead developer of CISO of Head IT. Of je bent bestuurder of directielid en je voelt je kwetsbaar: jij wil met jouw business niet in het nieuws komen zoals de supermarkten met de kaashack of Universiteit Maastricht.

Wat in bijna elk bedrijf onderschat wordt, is dat de grootste kwetsbaarheden ontstaan als je niet op het juiste niveau beveiligt. Dit is ook waarom generieke tools levensgevaarlijk zijn: ze vertellen je alleen globaal wat de risico's zijn.

Maar met globaal kom je er niet. Want een hacker denkt specifiek. Die heeft laserfocus.

De checklist die jij nu voor je hebt, helpt je om op het juiste niveau keuzes te maken. Zodat je niet onnodig overbeschermd bent, met eeuwig oplopende kosten (en hoofdpijn!) van dien. Maar ook niet onderbeschermd, waardoor je onnodige risico's neemt. Want wat je niet weet, creëert onvoorziene ellende & wat je niet hoeft te weten, creëert onnodige stress.

0

STAP 0. LEIDERSCHAP

Ben jij lead developer, CISO of Head IT? Zorg dan eerst dat het dagelijks bestuur of directie en management aan boord is, voordat je begint aan deze checklist. Zij zullen leiderschap moeten tonen en daadwerkelijk verantwoordelijkheid nemen voor de digitale weerbaarheid van jullie organisatie.

1

STAP 1. INZICHT CREËREN

doe dit samen met het dagelijks bestuur of directie en management

- ✔ Wat zijn je bedrijfskritische processen? Waar kan je geen dag of geen uur zonder?
- ✔ In welke keten zit je?
- ✔ Wat heb je aan services en knooppunten draaien? Denk aan rechtstreekse lijnen tussen databases met medische of financiële gegevens. Objecten die jij op afstand beheert: sluizen, toegangssystemen, toezichtcamera's.
- ✔ Wat verwachten stakeholders van jouw veiligheid en hun data?
- ✔ Wat zijn de consequenties als onbevoegden hier toegang tot hebben en van binnenuit kunnen manipuleren, zoals het plaatsen van ransomware? Wat is de reikwijdte van die consequenties?
- ✔ Hoe 'rank' je de aantrekkelijkheid van jouw data?
- ✔ Welke reële risico's loop je?

Jouw keten: wie zijn je klanten, partners en leveranciers? Heb je bouwtekeningen van interessante objecten (gevangenissen, lab, boorplatform)? Staan er financiële gegevens van een beursgenoteerde organisatie in jouw systemen? Produceer je in opdracht van een klant producten met intellectueel eigendom? Ben je voorraadhoudend voor retailorganisaties?

2

STAP 2. BLINDE VLEKKEN INZICHTELIJK MAKEN

- ✔ Hoe hebben we de risico's die we niet willen/kunnen lopen, afgedekt?
- ✔ Zoek contracten op: wat zijn de voorwaarden? Zitten hun cybersecuritymaatregelen minimaal op hetzelfde niveau als die van ons?
- ✔ Bel je business critical-leveranciers op: wat kunnen we verwachten als het misgaat? Denk aan internetverbindingen, toegangsbeheersystemen en externe IT-organisatie(s).
- ✔ Vraag leveranciers om systemen die zij voor je beheren na te lopen op ernstige kwetsbaarheden.
- ✔ Wat hebben we afgesproken met onze softwareleveranciers over incidentresponse?
- ✔ Wat is de uptime-garantie?
- ✔ Wat doen we als we die uptime niet halen?

Bonusvraag: hoe kun jij hier waarde in creëren? Want dit is een klapstuk voor de communicatie met je cliënten of gebruikers, als jij kunt aantonen dat jij je netwerk en infrastructuur zo hebt ingeregeld dat je kunt garanderen dat je hun gegevens optimaal beveiligd hebt tegen datalekken met een bepaalde uptime-garantie.

3

STAP 3. KORTE TERMIJNPLAN

je voorbereiden op een incident

- ✔ Wie zijn de belangrijke interne stakeholders die in actie moeten komen als er iets gebeurt?
- ✔ Wie doet wat wanneer en met welke prioriteit? Tot op het niveau van: wie kan deze server opnieuw opstarten?
- ✔ Wie beheert de telefoonlijst?
- ✔ Hoe tuigen we de 'belboom' op?
- ✔ Wie is onze externe cybersecurity-adviseur en wat is de speeddial hiervoor?
- ✔ Hoe zetten we data terug en hebben we dit getest?
- ✔ Waar slaan we dit plan op? Letterlijk: wie heeft toegang tot het papierje in welke kluis?
- ✔ In welke volgorde brengen we services up of down als er op welk knooppunt iets gebeurt?

Hoe één gehackt wachtwoord een sneeuwbal effect kan creëren? Een hack op een [oliepijplijn in Amerika](#) zorgde niet alleen voor rijen bij benzinstations, maar ook dat de wetgeving snel werd aangepast en dat het Witte Huis meteen in actie kwam om Rusland onder druk te zetten.

4

STAP 4. TOETS JE RISICOBEELD

- ✔ Wat is ons aanvalsoppervlak? Hoe kijken hackers naar ons?
- ✔ Zijn al onze blinde vlekken in kaart gebracht?
- ✔ Is er een helder overzicht van relevante securityrisico's en dure dreigingen?
- ✔ Hebben we een duidelijk beeld van tegen welke dreigingen we ons moeten beschermen (threat intelligence)? Is dat nog niet duidelijk, laat ons je dan helpen met een pentest. Dan weet je precies hoe ver een hacker in jouw netwerk kan binnendringen én hoe je je er tegen kunt beschermen. Handig!

5

STAP 5. OPTIMALISATIE

- ✔ Hebben we realtime inzicht in kwetsbaarheden en incidenten? Als dat realtime inzicht trouwens nog niet hebt... Wij helpen je hier graag mee. Plan een gratis strategiesprek in en we vertellen je alles!
- ✔ Monitoren we continu de juiste zaken om het aanvalsoppervlak (verder) te verkleinen?
- ✔ Zijn de cybersecuritymaatregelen optimaal en duurzaam ingericht?
- ✔ Missen we specifieke cybersecuritymaatregelen?
- ✔ Plan een periodieke toetsing in en een proces: voldoen de huidige maatregelen nog tegen de actuele dreigingen? En, zijn we het nog eens met de geaccepteerde risico's?

6

STAP 6. LANGETERMIJNANPAK

- ✔ Wordt de gekozen strategie regelmatig geëvalueerd en zo nodig bijgesteld?
- ✔ Is er een volledige incidentdetectie en response, 24/7?
- ✔ Koppel die met een (extern) security operations center (SOC). Kunnen we aan alle stakeholders aantonen dat we bewezen goed beveiligd zijn?
- ✔ Zijn de cybersecuritymaatregelen geprofessionaliseerd in een informatiebeveiligingsbeleid met de daarbij behorende processen en procedures? Pssst... Een hint van onze Robin Hoods: hanteer hiervoor de ISO27001, de standaard in informatiebeveiliging. Overweeg ook om je organisatie te laten certificeren voor deze ISO27001.

ALLE STAPPEN DOORLOPEN?

Je hebt nu een eerste stap gezet in de basishygiëne, en hebt inzicht verkregen in je cybersecuritymaatregelen en kwetsbaarheden binnen je organisatie.

Als het goed is heb je nu in kaart op welk niveau jouw business zit als het gaat om basishygiëne. Je kunt nu op het juiste niveau beslissingen nemen en je beveiliging steeds een level 'volwassener' maken. Anders gezegd: nu kun je steeds precies de juiste zaken oplossen.

Klaar om je beveiligingshygiëne hoger te tillen dan het basisniveau? Plan dan nu een gratis strategiesprek in en laat je persoonlijk door een van onze Robin Hoods adviseren over welke stap op dit moment voor jou en jouw organisatie het meest waardevol is.

Ja, ik wil uitstijgen boven de basishygiëne

SECWATCH