CYBERVEILIG NEDERLAND

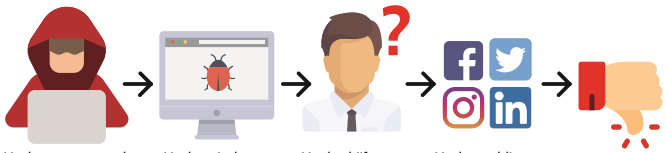
Hoe krijg je hulp van ethische hackers?

Als belangenvereniging van de Nederlandse cybersecurity-sector wil Cyberveilig Nederland de digitale weerbaarheid van ons land vergroten. Hiertoe is het essentieel dat ICT-kwetsbaarheden snel worden opgespoord en verholpen. De inzet van ethische hackers is hiervoor een waardevol instrument. Zij kunnen met hun grote technische kennis, inzet en kritische blik het internet veiliger maken. Deze hackers gaan vaak op zoek naar kwetsbaarheden, en wanneer ze die vinden, willen ze die melden bij de betreffende organisatie. Als dat jouw organisatie is, ben je gebaat bij het goed in ontvangst nemen van deze informatie!

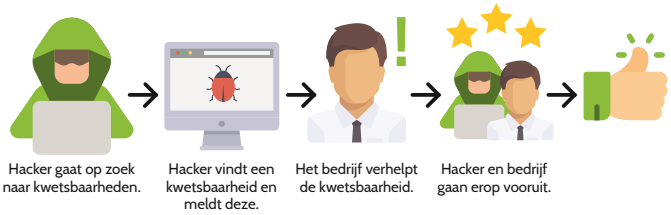
Om de inzet van ethische hackers te stimuleren onderschrijven de leden van Cyberveilig Nederland een Coordinated Vulnerability Disclosure (CVD) beleid, en hanteren zij deze werkwijze. Zo'n beleid geeft de spelregels aan waaraan ethische hackers zich moeten houden bij het melden van kwetsbaarheden in IT. Hackers worden uitgenodigd om binnen bepaalde grenzen, kwetsbaarheden die ze vinden bij je te melden.

Zo'n beleid op je website is een goede start, maar wat doe je als een kwetsbaarheid gemeld wordt? Om er voor te zorgen dat het niet blijft bij goede bedoelingen en dat gemelde kwetsbaarheden ook daadwerkelijk aangepakt worden, heeft Cyberveilig Nederland nu een eenvoudig stappenplan ontwikkeld. Een stappenplan waarmee elke organisatie, groot of klein, CVD kan inzetten voor het veiliger maken van de eigen ICT-omgeving.

Geen beleid
Gefrustreerde hacker en imagoschade voor het bedrijf.



CVD-beleid
Gewaardeerde hacker en security-verbetering voor het bedrijf.



De 6 stappen voor het succesvol inzetten van CVD:

1. Regel mandaat en commitment van het management.
2. Inventariseer je IT.
3. Besluit over zelf doen of uitbesteden.
4. Maak een proces voor wat te doen bij een melding.
5. Plaats een tekst met CVD-beleid op je website.
6. Test en blijf testen.

STAP 1

Het opzetten van een Coordinated Vulnerability Disclosure (CVD) beleid is vaak het domein van de (Chief) Information Security Officer (CISO), CIO of ICT Manager. Overleg voor een effectief en breed gedragen CVD-aanpak ook met:

- Management. Wie is verantwoordelijk en aan wie geeft het management het mandaat om het CVD-beleid in te richten?
- IT. Is de juiste IT-kennis en capaciteit in huis om (tijdig) meldingen af te handelen en op waarde te schatten?
- Juridisch. Meldingen kunnen juridische implicaties hebben voor de organisatie en de melder.
- Communicatie. Het niet juist afhandelen van CVD kan invloed hebben op het imago van de organisatie. Ook interne communicatie over meldingen moet goed worden afgestemd.
- Financiën. Indien je van plan bent een beloning uit te keren bij meldingen.

STAP 2

Als een melding binnen komt, moet het betreffende IT-systeem waarschijnlijk aangepast worden om de gemelde kwetsbaarheid te verhelpen. Het is dus belangrijk om van alle IT-systemen te weten:

- Wie is er verantwoordelijk voor?
- Wie kan wijzigingen uitvoeren?
- Hebben we een externe leverancier nodig, zoals een cloud- of software-leverancier? Zo ja, dan moeten daar afspraken mee gemaakt worden.

STAP 3

Maak een afweging of je als organisatie zelf de beoordeling van binnenkomende meldingen wilt voeren of dit wilt uitbesteden aan gespecialiseerde cybersecurity dienstverleners. Bij het beoordelen van de ernst en impact van een melding kan technische security-expertise vereist zijn, en niet elke organisatie heeft die in huis. Verschillende leden van Cyberveilig Nederland bieden zo'n dienstverlening aan.

Als je het zelf wilt doen zorg dan dat je voldoende IT-kennis en security-kennis in huis hebt om de meldingen op waarde in te schatten en meldingen goed af te handelen. Hierbij is het belangrijk dat je de taal van de hackers spreekt.

STAP 4

Richt het proces van de (vaak technische) communicatie met de melder zorgvuldig in.

- Maak een mailadres aan waar meldingen kunnen binnenkomen
- Zorg dat informatie-uitwisseling met de melder vertrouwelijk kan plaatsvinden via een versleutelde verbinding, bijvoorbeeld PGP;
- Gebruik een template om de melder om nadere informatie te vragen;
- Maak een logbestand aan en houd daarin de voorgang en taakverdeling van de melding bij;
- Bepaal binnen hoeveel dagen op een melding wordt gereageerd en communiceer dit met de betrokken personen binnen je organisatie;
- Communiceer met de melder hoeveel tijd je nodig hebt om de melding te analyseren en op te lossen.

Verder is het verstandig om te inventariseren welke bestaande crisis- of incident-responsprocedures er al zijn binnen de organisatie. Het te ontwikkelen CVD-proces kan hier mooi op meeliften.

STAP 5

Maak zelf een tekst of gebruik een tekst van bijvoorbeeld het responsibledisclosure.nl die je aanpast aan jouw wensen en spelregels. Denk bijvoorbeeld na of je je CVD-beleid in het Nederlands of in het Engels wilt opzetten. Meldingen in het Nederlands voorkomen veel 'ruis'-meldingen uit niet-Nederlandstalige landen. Echter je sluit dan wel een grote gemeenschap van Engelstalige ethische hackers uit. Stel ook vast hoe je de meldingen wilt belonen. Dat kan met geld maar ook een plek op de Wall of Fame van de organisatie is voor veel (ethische) hackers vaak al genoeg.

Het is belangrijk dat je de beloften die je in het beleid doet (zoals geen strafrechtelijke vervolging najagen), ook waar kan maken. Zorg dus dat je goed aangeeft wat de grenzen zijn waarbinnen de ethische hacker moet blijven wil hij binnen het beleid vallen. Ook is het belangrijk dat je goed aangeeft welke systemen wel en niet binnen de scope van het beleid vallen.

STAP 6

Test de procedures door zelf een CVD-melding te doen en te zien of het proces werkt zoals beoogd. Als er geen meldingen binnenkomen, doe dan ten minste jaarlijks een oefening om het proces levend te houden binnen de organisatie.

Computest always on. FOX IT FOR A MORE SECURE SOCIETY HackDefense kiwa Secura zerocopter NORTHWAVE Intelligent Security Operations

Tot stand gekomen met experts van bovenstaande leden. Productie door Computest. Mede mogelijk gemaakt door Chris van 't Hof