

Hack-check

Geeft inzicht in online risico's



In 2018 gaf 8,5 procent van de internetgebruikers van 12 jaar of ouder aan in de afgelopen twaalf maanden slachtoffer te zijn geweest van digitale criminaliteit. Dat komt neer op ruim 1,2 miljoen mensen! Door het toenemende gebruik van IT en IT-dienstverlening neemt het aantal slachtoffers verder toe. Het weerbaar maken van potentiële slachtoffers is een belangrijk en effectief middel in het voorkomen van cyberincidenten. Maar hoe breng je bewustwording van cybercrime op en leuke, interactieve en pragmatische wijze onder de aandacht? Met de Hack-check!

Het uitgangspunt van de Hack-check is dat deelnemers zich bewust worden van de risico's die samenhangen met het gebruik van IT en hoe deze risico vaak op simpele wijze ondervangen kunnen worden. De Hack-check is een effectief middel waarmee de deelnemers op laagdrempelige wijze inzicht verkrijgen in welke risico's zij lopen bij het gebruik van internet. De check bestaat uit verschillende interactieve elementen die enerzijds bedoeld zijn om de deelnemer te informeren en anderzijds om ze op leuke wijze te confronteren met "risicovol gedrag".

Onderdelen Hack-check

De Hack-check kan helemaal op maat gemaakt worden voor de opdrachtgever. De hackers hebben een breed scala aan activiteiten die zij uitvoeren en kunnen laten zien. Denk hierbij aan:

1. Meet the hacker

Deelnemers hebben de mogelijkheid daadwerkelijk een hacker te ontmoeten en te spreken over zijn/haar activiteiten. De hackers geven uitleg over manieren waarop burgers kwetsbaar zijn voor cybercriminelen.

2. Social media quick-scan

Als deelnemers het aandurven dan kunnen zij hun naam achterlaten op een formulier (na eerst toestemming te hebben gegeven) om door één van de experts hun social media en internetactiviteiten te laten onderzoeken. De hackers voeren gedurende 30 minuten een quick-scan uit en proberen zoveel mogelijk openbaar beschikbare informatie over de deelnemer te achterhalen. Op basis van de gevonden informatie ontvangt de bezoeker alle informatie die we online over hem of haar hebben kunnen vinden. Tegelijkertijd geven de experts tips om internetactiviteiten en social media beter af te schermen of te beveiligen.

3. Demonstraties

De experts van de Hack-check zijn in staat om op gezette momenten een aantal demonstraties te geven van voor de

hand liggende of juist complexere manieren waarop zij zichzelf toegang kunnen verschaffen op het device van hun doelwit. Denk hierbij aan:

- **Rubber Ducky-demo**

Bij de Rubber Ducky-demo mag een bezoeker de USB stick in één van de laptops steken. Een Rubber Ducky zal dan per direct een script initiëren op de laptop, het effect hiervan wordt weergegeven op een groot scherm in de stand. Deze demonstratie leert bezoekers dat zij nooit zomaar een onbekende USB stick in hun PC moeten steken.

- **Misbruik van de Bluetoothmodule**

Bij deze demonstratie laten de experts zien hoe een hacker zichzelf toegang kan verschaffen tot een laptop die niet op een netwerk is aangesloten, door gebruik te maken van de Bluetoothmodule. Dit leert bezoekers om ook waakzaam te zijn op momenten dat zij geen internetverbinding hebben, maar wel Bluetooth hebben ingeschakeld.



- **Passief af luisteren wifi**

Door gebruik te maken van een door de experts geconfigureerde wifi-receiver, worden de wifi-netwerken van de deelnemers weergegeven. Dit geeft de experts inzicht in waar de deelnemers de afgelopen tijd geweest zijn. Hiervoor is toestemming nodig van de deelnemers en wegens privacy redenen zal dit niet op een groot scherm worden weergegeven. Dit leert deelnemers veilig gebruik te maken van (openbare) wifi-netwerken.

- **Malicious app demo**

De experts bouwen een kleine malicious Android app die 'volledige' controle geeft over het device van de deelnemer. Deze app kan simpel worden geïnstalleerd door het scannen van een QR code door de gebruiker. Mocht een deelnemer het aandurven dan mag hij/zij de applicatie downloaden onder begeleiding van een hacker. Na afloop van de demo wordt de applicatie volledig verwijderd van het apparaat van de gebruiker.

- **Security en Privacy Quiz**

Deelnemers krijgen verschillende vragen voorgeschoteld om het bewustzijn te vergroten. Alle deelnemers krijgen een deelnamecertificaat en maken kans op het winnen van een goodiebag.



INTERESSE?

Ben je benieuwd naar de ervaringen van een gemeente met de Hack-check? Dat kan, want Almere heeft de Hack-check meerdere keren ingezet. Neem hiervoor contact op met Annemien Poortier via ahpoortier-vhouten@almere.nl.

Gemeente Almere

