Hacking / Sabotage

PDF Versie

Wat is Hacking / Sabotage ?

Hacking:

Is het ongeoorloofd binnendringen in een computersysteem. Met de inbraak is meestal kwaad opzet gemoeid, maar ook onopzettelijk een verbinding tot stand brengen en die verbinding vrijwillig behouden, wordt als hacking beschouwd. Zelfs het hacken van een informaticasysteem dat niet of nauwelijks beveiligd is, is strafbaar.

Data- en informaticasabotage:

Informaticasabotage is het best te omschrijven als vandalisme in een informaticaomgeving.
Het verschil met informaticabedrog is dat informaticasabotage geen verrijking tot gevolg hoeft te hebben. Gegevens zonder toestemming wijzigen, is op zichzelf al een misdrijf.

Ook het ontwikkelen en verspreiden van datasabotagetools is strafbaar.

Wat heb je nodig om klacht neer te leggen?

- Verzamel informatie over het gehackte toestel
    - Merk en model, serienummer, besturingssysteem, anti-virusprogramma, ...
    - Wie heeft toegang (zowel fysiek als vanop afstand) tot het toestel
    - Wanneer werkte het toestel correct en wanneer werd het probleem vastgesteld, op welke wijze en door wie

    - Wat heeft zich voorgedaan vlak voor het probleem (op een link geklikt, een boodschap gekregen op het scherm, ...)
    - Hebt u hulp ingeroepen van een expert? Vraag deze dan om zoveel mogelijk bewijsmateriaal af te drukken of te downloaden zodat u dit ons kan overhandigen. *Bijvoorbeeld logbestanden*.
- Verzamel informatie omtrent de eventuele communicatie met de dader
    - telefoonnummers, e-mailadressen, (scherm)namen, IP-adressen, gebruikte sociale media accounts, ...
    - neem schermafdrukken
- Verzamel informatie omtrent de eventuele betalingen
    - rekeningnummers, transacties, bitcoin-adressen, ...
    - neem schermafdrukken

Wat kan je nog doen?

- Verander uw wachtwoorden van al uw accounts.
- Activeer tweestapsverificatie (2FA) voor **elke account die dit ondersteunt.**
    - Hierdoor kunnen hackers geen toegang nemen tot uw account, ook al beschikken zij over je login en wachtwoord. er moet immers nog een "tweede stap" ondernomen worden. Dit kan via SMS of een app op je smartphone
- Controleer je computer of toestel op virussen en spyware door een uitgebreide scan uit te voeren. Bij twijfel, contacteer een expert.
- Beperk de schade door al uw toestellen van het internet los te koppelen (denk ook aan Wifi-verbindingen)

Hoe vermijd je om opnieuw slachtoffer te worden?

- Gebruik veilige wachtwoorden (lang, met cijfers, symbolen, kleine letters en hoofdletters, het kan ook een zin zijn).
- Gebruik “two factor authentication” waar mogelijk. Dit is een bijkomende beveiliging via bijvoorbeeld uw gsm.
- Gebruik voor elke belangrijke account een uniek wachtwoord, deel het niet en vermeld de wachtwoorden niet in uw e-mails, smartphone of computer.
- Beveilig uw computersystemen door een antivirussoftware, een firewall en anti-spyware te installeren en voer regelmatig een scan uit.
- Installeer regelmatig de updates van uw computer en uw programma’s. U kan dit instellen dat dit automatisch gebeurt zodra de update beschikbaar

is.

- Blijf kritisch ten opzichte van e-mails van onbekende afzenders. U kunt deze beter niet openen, noch beantwoorden of doorsturen.
- Download geen software of iets anders van onbekende bronnen.
- Wanneer u bent ingelogd op een website om aankopen te doen, een commentaar of iets anders te schrijven, denk er dan aan u af te melden voordat u de pagina verlaat.
- Vraag advies bij twijfel!

Waar vind je meer informatie?

https://www.safeonweb.be/nl/mijn-account-gehackt