Overname sociale media/website/mailbox

Version PDF

Wat is de overname van een profiel op sociale media/een website of een mailbox ?

Deze inbreuk kan meerdere vormen aannemen :

je hebt geen toegang meer tot je account / online profiel / mailbox en / of je merkt dat iemand er kennelijk toegang toe heeft gehad zonder je toestemming.

of

Iemand gebruikt je account / online profiel / mailbox om namens jou berichten te verzenden of te posten.

In het algemeen spreken we van een inbreuk op de vertrouwelijkheid, integriteit en beschikbaarheid van computersystemen en gegevens die door deze systemen worden opgeslagen, verwerkt of verzonden *(Hacking)*.

Als de inhoud van het online account/profiel, de mailbox, de website, ... wordt gewijzigd, gewist of zelfs buiten gebruik wordt gesteld, dan spreken we over data- en informaticasabotage.

Dit type feit kan zich afspelen in een persoonlijke context (geweld binnen het gezin, pesterijen, professionele conflicten, enz.) maar meestal is het het werk van een verdachte die zijn slachtoffers willekeurig uitkiest, naar gelang de "opportuniteiten" die zich voordoen. Je moet je dus niet persoonlijk of direct geviseerd voelen.

Wat heb je nodig om klacht neer te leggen?

Indien mogelijk, gelieve nota te nemen van de volgende sporen en elementen:

- De exacte URL (internetadres) van de site/account/het profiel in kwestie;
- De unieke ID van de betrokken site/account/profiel;
- Indien mogelijk, een screenshot van de betreffende pagina of het bericht;
- Uw e-mail adres;
- De exacte datum en tijd van deze gebeurtenis;
- Overzicht van de elementen die aantonen dat iemand zich zonder toestemming toegang heeft verschaft tot uw e-mailbox (bv. account ontoegankelijk, berichten verzonden in uw naam, berichten verwijderd zonder uw toestemming,...);
- Datum, tijd, tijdzone en IP-adres van de laatste verbindingen met de mailbox, indien beschikbaar (alleen beschikbaar indien u nog toegang heeft tot de mailbox);
- Foto's of screenshots van de sporen die de "hacker" heeft achtergelaten.
- Datum, tijdstip en tijdzone van het gesprek of de gesprekken die u met de verdachte(n) hebt gevoerd;
- Inhoud van de door de verdachte verzonden e-mails (bij te voegen) + volledige technische header (https://mxtoolbox.com/public/content/emailheaders/);
- Beschrijving van de op verzoek van de verdachte verrichte handelingen;

Wat kan je nog doen?

- Waarschuw al je contacten, zodat zij niet door de verdachte in de val worden gelokt;
- Start het antivirusprogramma op het geïnfecteerde apparaat, maar ook op al uw aangesloten apparaten (smartphone, tablet, computer, ...);
- Verander de wachtwoorden voor al uw accounts (zelfs diegene die niet lijken te worden beïnvloed);
- Wijzig uw beveiligingsvragen;
- Schakel indien mogelijk de tweestapsverificatie in;
- Neem contact op met de serviceprovider van uw profiel / e-maildienst als u door de hacking geen toegang meer geeft;
- Veelal zijn er herstelopties beschikbaar.

Hoe vermijd je om opnieuw slachtoffer te worden?

Om te voorkomen dat je weer slachtoffer wordt van dit soort gebeurtenissen,

- Zorg ervoor dat u de beveiligingsregels voor toegang tot uw online bronnen effectief configureert.
- Activeer de verbinding via dubbele authenticatie (2FA) wanneer deze optie wordt voorgesteld.

Waar vind je meer informatie?

U zou meer informatie moeten kunnen vinden op de "Help/Helpdesk" pagina of in de beveiligingsopties van de betreffende dienst/website.