Forensische Tijdlijn – WordPress Indringer

Dit document bevat een forensische tijdlijn en analyse van een digitale inbraak in een betaald WordPress-account, waarbij een anoniem account ('brisklybeare49084e6c6') werd aangemaakt met misbruik van het e-mailadres info@corawesterink.com.

1. Voorafgaande gebeurtenissen (2014–2023)

- 2014–2020: Herhaald digitaal misbruik van persoonsgegevens, e-mailadressen en sociale media.
- 2020: Politiedossier verwijderd, sleutelgebeurtenis in digitale sabotage.
- April 2023: Officiële klacht ingediend bij FBI/IC3 vanwege misbruik van IP-adres en e-mailaccounts.

2. Aanmaak van het valse account (April 2025)

In WordPress werd het account 'brisklybeare49084e6c6' aangemaakt en gekoppeld aan het e-mailadres info@corawesterink.com. Dit wijst op misbruik van e-mail of IP-adres. Het account werd geregistreerd in April 2025.

3. Vestigen van controle

Na registratie kon de indringer inloggen in het WordPress-dashboard, toegang krijgen tot instellingen en blogs, en mogelijk aanvullende beheerdersrechten genereren. Hiermee ontstaat een schaduw-identiteit gekoppeld aan het domein.

4. Potentiële acties door de indringer

1. Manipulatie van blogs (verwijderen, aanpassen, nepberichten plaatsen).
2. Digitale identiteitsfraude (nieuwe accounts elders aanmaken, doen alsof hij/zij de eigenaar is).
3. Financieel misbruik (facturen of betaalgegevens manipuleren).
4. Sabotage van reputatie en bereik (blogs blokkeren, bezoekers omleiden).

5. Relevantie voor strafrechtelijk onderzoek

Dit betreft herhaald delictgedrag: hetzelfde modus operandi is in 2023 al gemeld bij de FBI.
Mogelijke strafbare feiten:

- Computervredebreuk (art. 138ab Sr).

- Identiteitsfraude (art. 231 Sr).
- Valsheid in geschrifte (art. 225 Sr).
- Fraude met betaalgegevens.

6. Concrete bewijzen (uit screenshot)

- Gebruikersnaam indringer: brisklybeare49084e6c6
- Join-datum: April 2025
- Misbruikte e-mailadres: info@corawesterink.com
- Platform: WordPress.com (Automattic Inc.)
- Locatie log: Account Settings > Username + Email Address

7. Aanbevolen vervolgstappen

1. Veiligstellen bewijzen (screenshots, metadata, logs).
2. Melding doen bij politie, FBI/IC3 en Automattic/WordPress Legal & Security.
3. Preventieve maatregelen: 2FA instellen, forwarding-regels controleren, onbekende sites verwijderen.