



Afwegingskader dreigingsinformatie voor ad hoc notificeren

Criteriachecklist:

- Is er een timestamp aanwezig?
- Is er een IP-adres aanwezig?
- Wat voor kwetsbaarheid, malware of zwakheid is het (wat is de context van de data)?
- Hoe is de data verkregen (bijv. scan methode, gaat het om gestolen data, etc)?
- Is er een handelingsperspectief mogelijk?
- Is de bron betrouwbaar (bijv. kennen we de bron)?
- Is de aangeleverde data valide (bijv. zitten er inconsistenties in, veel false positives, etc)?
- Is de data bedoeld voor notificaties?

Toelichting

Data moet bij voorkeur niet ouder dan een maand oud zijn. Afhankelijk van de ontvanger (doelgroep) van de data, kan hier een andere inschatting voor worden gemaakt.

Toelichting

Is er bijvoorbeeld malware of ransomware of een achterdeur aanwezig op het systeem die toegang biedt aan kwaadwillenden?

Toelichting

Is het systeem een actief doelwit van bijvoorbeeld een DDoS-aanval of (significante) andere aanvallen?

Toelichting

Is het systeem bijvoorbeeld onderdeel van een botnet, of ingericht om brute force, DDoS of andere aanvallen uit te voeren op derden systemen?

Andere criteria:

- Is het systeem kwetsbaar voor een kwetsbaarheid met CVSS score ≥ 8.8 , en/of;
- Wordt er een exploit verwacht (wordt het product bijv. veel gebruikt), en/of;
- Is er veel media- of politieke aandacht (onrust) voor de geconstateerde kwetsbaarheid of zwakheid en/of;
- Heeft de kwetsbaarheid, misconfiguratie of zwakheid als direct gevolg het lekken van (potentieel) gevoelige gegevens, en/of;
- Is de data extra relevant voor een specifieke doelgroep van NCSC / CSIRT-DSP / DTC?

Bijvoorbeeld:

- Lijsten die gedeactiveerd zijn door de bron;
- Lijsten die al tijden geen data meer opleveren.

